



DASAR KESELAMATAN ICT (DKICT)


VERSI 3.0

PENTADBIRAN KERAJAAN
NEGERI SEMBILAN

ISO/IEC 27001:2013

PENGURUSAN SISTEM KESELAMATAN MAKLUMAT



	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

ISI KANDUNGAN


SEJARAH DOKUMEN	1
REKOD PINDAAN.....	2
PENGENALAN	3
OBJEKTIF.....	3
PERNYATAAN DASAR	4
SKOP.....	6
PRINSIP-PRINSIP	10
PENILAIAN RISIKO KESELAMATAN ICT	13
BIDANG 01 PEMBANGUNAN DAN PENYELENGGARAAN DASAR	16
0101 Dasar Keselamatan ICT.....	16
010101 Pelaksanaan Dasar.....	16
010102 Penyebaran Dasar	16
010103 Penyelenggaraan Dasar	17
010104 Pematuhan Dasar	18
BIDANG 02 ORGANISASI KESELAMATAN	19
0201 Struktur Organisasi Dalam.....	19
020101 Setiausaha Kerajaan Negeri Sembilan	19
020102 Ketua Pegawai Maklumat (CIO)	20
020103 Pegawai Keselamatan ICT (ICTSO)	21
020104 Pegawai Keselamatan Jabatan (PKJ).....	23
020105 Pengurus ICT	25
020106 Pentadbir Sistem ICT	27
020106A Pentadbir Rangkaian & Keselamatan.....	27
020106B Pentadbir Pangkalan Data.....	29
020106C Pentadbir Laman Web (Webmaster)	29
020106D Pentadbir Pusat Data/Bilik Server	30
020106E Pentadbir Sistem Aplikasi.....	31
020106 Pentadbir Rangkaian & Keselamatan	31
020106 Pentadbir Emel	32
020107 Pegawai Aset.....	33
020108 Pengguna	34

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


020109	Jawatan Kuasa Pemandu ICT Negeri Sembilan (JPICIT).....	37
020110	Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan.....	40
	Negeri Sembilan (CERTNS)	
0202	Pihak Luaran	43
020201	Keperluan Keselamatan Kontrak dengan Pihak Luaran	43
BIDANG 03	PENGURUSAN ASET	45
0301	Akauntabiliti Aset	45
030101	Inventori Aset ICT	45
0302	Pengelasan dan Pengendalian Maklumat	46
030201	Pengelasan Maklumat	47
030202	Pengendalian Maklumat	47
BIDANG 04	KESELAMATAN SUMBER MANUSIA	49
0401	Keselamatan Sumber Manusia Dalam Tugas Harian	49
040101	Sebelum Perkhidmatan.....	49
040102	Dalam Perkhidmatan	50
040103	Bertukar Atau Tamat Perkhidmatan.....	52
040104	Program Kesedaran Keselamatan ICT	53
BIDANG 05	KESELAMATAN FIZIKAL DAN PERSEKITARAN.....	54
0501	Keselamatan Kawasan.....	54
050101	Kawalan Kawasan	54
050102	Kawalan Masuk Fizikal	56
050103	Kawasan Larangan	56
0502	Keselamatan Peralatan	58
050201	Peralatan ICT.....	59
050202	Media Storan	62
050203	Media Tandatangan Digital	64
050204	Media Perisian dan Aplikasi (<i>Software</i>)	65
050205	Penyelenggaraan Perkakasan.....	66
050206	Peralatan di Luar Premis	67
050207	Pelupusan Perkakasan	68
0503	Keselamatan Persekitaran.....	70
050301	Kawalan Persekitaran	70
050302	Bekalan Kuasa.....	72
050303	Kabel Komputer/ Rangkaian	72
050304	Prosedur Kecemasan	73
0504	Keselamatan Dokumen	74
050401	Dokumen	74

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


BIDANG 06	PENGURUSAN OPERASI DAN KOMUNIKASI	76
0601	Pengurusan Prosedur Operasi.....	76
060101	Pengendalian Prosedur	76
060102	Kawalan Perubahan.....	76
060103	Pengasingan Tugas dan Tanggungjawab.....	77
0602	Pengurusan Penyampaian Perkhidmatan Pihak Luaran.....	78
060201	Penyampaian Perkhidmatan.....	78
0603	Perancangan dan Penerimaan Sistem.....	79
060301	Perancangan Kapasiti.....	79
060302	Penerimaan Sistem.....	80
0604	Perisian Berbahaya	80
060401	Perlindungan daripada Perisian Berbahaya.....	81
060402	Perlindungan daripada <i>Mobile Code</i>	82
0605	Housekeeping.....	82
060501	<i>Backup</i>	82
0606	Pengurusan Rangkaian.....	83
060601	Kawalan Infrastruktur Rangkaian.....	83
0607	Pengurusan Media.....	84
060701	Pengendalian Media	85
0608	Pengurusan Pertukaran Maklumat	85
060801	Pertukaran Maklumat.....	86
060802	Pengurusan Mel Elektronik (E-mel)	86
0609	Perkhidmatan Pembayaran Dalam Talian	87
060901	Pembayaran Atas Talian.....	87
0610	Pemantauan	88
061001	Pengauditan dan Forensik ICT	88
061002	Jejak Audit	89
061003	Sistem Log.....	90
061004	Pemantauan Log.....	90
BIDANG 07	KAWALAN CAPAIAN	93
0701	Dasar Kawalan Capaian.....	93
070101	Keperluan Kawalan Capaian	93
0702	Pengurusan Capaian Pengguna	94
070201	Akaun Pengguna	94
070202	Hak Capaian	95
070203	Pengurusan Kata Laluan	96
070204	<i>Clear Desk</i> dan <i>Clear Screen</i>	97

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

0703	Kawalan Capaian Rangkaian.....	98
070301	Capaian Rangkaian	98
070302	Capaian Internet	99
0704	Kawalan Capaian Sistem Pengoperasian.....	100
070401	Capaian Sistem Pengoperasian	100
070402	Capaian Pihak Luaran	101
0705	Kawalan Capaian Data, Maklumat dan Sistem Aplikasi	102
070501	Capaian Data, Maklumat dan Sistem Aplikasi	102
0706	Peralatan Mudah Alih dan Kerja Jarak Jauh	103
070601	Peralatan Mudah Alih dan Kerja Jarak Jauh	103
BIDANG 08	PEROLEHAN PEMBANGUNAN & PENYELENGGARAAN ..	104
	SISTEM APLIKASI	
0801	Keselamatan Dalam Membangunkan Sistem Aplikasi	104
080101	Keperluan Keselamatan Sistem Aplikasi	104
080102	Pengesahan Data Input dan Output.....	105
0802	Kawalan Kriptografi.....	106
080201	Enkripsi	106
080202	Tandatangan Digital.....	106
080203	Pengurusan Infrastruktur Kunci Awam (PKI)	106
0803	Keselamatan Fail Sistem Aplikasi.....	107
080301	Kawalan Fail Sistem Aplikasi	107
0804	Keselamatan Proses Pembangunan dan Penyelenggaraan	108
080401	Prosedur Kawalan Perubahan	108
080402	Pembangunan Sistem Aplikasi Secara <i>Outsource</i>	108
0805	Kawalan <i>Vulnerability</i> Teknikal	109
080501	Kawalan Ancaman Teknikal.....	109
BIDANG 09	PENGURUSAN PENGENDALIAN INSIDEN	110
	KESELAMATAN ICT	
0901	Mekanisme Pelaporan Insiden Keselamatan ICT	110
090101	Mekanisme Pelaporan	110
0902	Pengurusan Maklumat Insiden Keselamatan ICT	112
090201	Prosedur Pengurusan Maklumat Insiden Keselamatan ICT	112
BIDANG 10	PENGURUSAN KESINAMBUNGAN PERKHIDMATAN	114
1001	Dasar Kesinambungan Perkhidmatan	114


	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

100101	Pelan Kesenambungan Perkhidmatan (PKP)	114
100102	Pelan Pemulihan Bencana (DRP).....	117
BIDANG 11	PEMATUHAN	120
1101	Pematuhan dan Keperluan Perundangan	120
110101	Pematuhan Dasar	120
110102	Pematuhan Dasar, Piawaian dan Prosedur	120
110103	Pematuhan Keperluan Audit	121
110104	Dokumen Perundangan	121
110105	Pelanggaran Dasar	121
GLOSARI.....		122
Lampiran 1	130
Lampiran 2	132
Lampiran 3	136
Lampiran 4	138
Lampiran 5	140

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


SEJARAH DOKUMEN

TARIKH	VERSI	KELULUSAN	TARIKH KUAT KUASA
23 MAC 2015	2.1	MESYUARAT JAWATANKUASA PEMANDU ICT (JPICT) KERAJAAN NEGERI SEMBILAN BIL.1/2015	23 MAC 2015
12 FEB 2019	3.0	MESYUARAT JAWATANKUASA PEMANDU ICT (JPICT) KERAJAAN NEGERI SEMBILAN BIL.1/2019	12 FEB 2019

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

REKOD PINDAAN

TARIKH	VERSI	BUTIRAN PINDAAN
12 FEB 2019	3.0	PINDAAN DOKUMEN DENGAN MERUJUK DASAR/PEKELILING/ SURAT ARAHAN SEDANG BERKUATKUASA DAN MENGAMBIL KIRA KEPERLUAN KESELAMATAN ICT SEMASA

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

PENGENALAN

Dasar Keselamatan ICT (DKICT) Pentadbiran Kerajaan Negeri Sembilan mengandungi peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset Teknologi Maklumat dan Komunikasi (ICT). Dasar ini juga menerangkan kepada semua pengguna mengenai tanggungjawab dan peranan mereka dalam melindungi Aset ICT di Pentadbiran Kerajaan Negeri Sembilan.


OBJEKTIF

DKICT Pentadbiran Kerajaan Negeri Sembilan diwujudkan untuk menjamin kesinambungan urusan Pentadbiran Kerajaan Negeri Sembilan dengan meminimumkan kesan insiden keselamatan ICT.

Dasar ini bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi Pentadbiran Kerajaan Negeri Sembilan. Ini hanya boleh dicapai dengan memastikan semua Aset ICT dilindungi.

Manakala, objektif utama Keselamatan ICT Pentadbiran Kerajaan Negeri Sembilan ialah seperti berikut:

- i. memastikan kelancaran operasi Pentadbiran Kerajaan Negeri Sembilan dan meminimumkan kerosakan atau kemusnahan;
- ii. melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi;

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


- iii. mencegah salah guna atau kecurian Aset ICT Kerajaan; dan
- iv. menyediakan ruang bagi penambahbaikan yang berterusan kepada pengurusan keselamatan dan pentadbiran ICT.

PERNYATAAN DASAR

Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Penjagaan keselamatan merupakan suatu proses yang berterusan. Ia melibatkan aktiviti berkala yang mesti dilakukan dari semasa ke semasa untuk menjamin keselamatan kerana ancaman dan kelemahan sentiasa berubah.

Keselamatan ICT adalah bermaksud keadaan di mana segala urusan menyediakan dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan ICT berkait rapat dengan perlindungan Aset ICT. Terdapat empat (4) komponen asas keselamatan ICT iaitu:

- i. melindungi maklumat rahsia rasmi dan maklumat rasmi kerajaan dari capaian tanpa kuasa yang sah;
- ii. menjamin setiap maklumat adalah tepat dan betul;
- iii. memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


- iv. memastikan akses hanya kepada pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

DKICT Pentadbiran Kerajaan Negeri Sembilan merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk menjamin keselamatan maklumat tersebut dan kebolehsediaan kepada semua pengguna yang dibenarkan.

Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

- i. kerahsiaan - maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran;
- ii. integriti - data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan;
- iii. tidak boleh disangkal - punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal;
- iv. kesahihan - data dan maklumat hendaklah dijamin kesahihannya; dan
- v. ketersediaan - data dan maklumat hendaklah boleh diakses pada bila-bila masa.

Selain itu, langkah-langkah ke arah menjamin keselamatan ICT hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan semula jadi Aset ICT; ancaman yang wujud akibat

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


daripada kelemahan tersebut; risiko yang mungkin timbul; dan langkah-langkah pencegahan sesuai yang boleh diambil untuk menangani risiko berkenaan.

SKOP

Aset ICT Pentadbiran Kerajaan Negeri Sembilan terdiri daripada perkakasan, perisian, sistem aplikasi, perkhidmatan, data, maklumat, manusia, media storan, dokumentasi, premis komputer dan peralatan rangkaian. DKICT Pentadbiran Kerajaan Negeri Sembilan menetapkan keperluan-keperluan asas berikut:

- i. data dan maklumat hendaklah boleh diakses secara berterusan dengan cepat, tepat, mudah dan boleh dipercayai. Ini adalah amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti; dan
- ii. semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta untuk melindungi kepentingan kerajaan, perkhidmatan dan masyarakat.

Bagi menentukan Aset ICT ini terjamin keselamatannya sepanjang masa, DKICT Pentadbiran Kerajaan Negeri Sembilan ini merangkumi perlindungan semua bentuk maklumat kerajaan yang diwujudkan, dimusnah, disimpan, dijana, dicetak, diakses, diedar dalam penghantaran dan yang dibuat salinan keselamatan. Ini akan dilakukan melalui pewujudan dan penguatkuasaan

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

sistem kawalan serta prosedur dalam pengendalian semua perkara-perkara berikut:

i. Perkakasan

Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan Pentadbiran Kerajaan Negeri Sembilan. Contoh komputer, pelayan, peralatan komunikasi, pencetak, media storan dan sebagainya;

ii. Perisian


Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan dalam sistem ICT. Contoh perisian aplikasi atau perisian sistem seperti :

- a. Sistem Pengoperasian (Windows, Linux, Ubuntu, Android);
- b. Sistem Pangkalan Data (MySQL, Oracle, MSSQL); dan
- c. Perisian Sistem Rangkaian dan Keselamatan (Antivirus, Firewall, BMT, DNS,DMS).

iii. Sistem Aplikasi

Satu program komputer yang dibangunkan bagi melakukan tugas pengguna secara spesifik untuk pengguna akhir (*end users*) yang menyediakan kemudahan pemprosesan maklumat kepada Pentadbiran Kerajaan Negeri Sembilan. Contoh sistem aplikasi seperti:

- a. Sistem HRMIS;
- b. Sistem e-Direktori; dan setaranya.

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

iv. Perkhidmatan

Perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan fungsi-fungsinya. Contoh:

- a. perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;
- b. sistem halangan akses seperti sistem kad akses; dan
- c. perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegah kebakaran, *Uninterruptible Power Supply* (UPS), *Close Circuit Television* (CCTV) dan lain-lain.

v. Data atau Maklumat


Koleksi fakta-fakta dalam bentuk kertas atau mesej elektronik, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif Pentadbiran Kerajaan Negeri Sembilan. Contohnya, sistem dokumentasi, prosedur operasi, rekod-rekod, profil-profil pelanggan, pangkalan data, fail-fail data, maklumat-maklumat arkib dan lain-lain;

vi. Manusia

Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja harian jabatan bagi mencapai misi dan objektif jabatan. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan;

vii. Media Storan

Semua media storan dan peralatan yang berkaitan seperti storan mudah alih, pita kartrij, CD-ROM, pita, cakera, pemacu cakera, pemacu pita dan lain-lain;

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

viii. Dokumentasi

Semua dokumen yang berkaitan dengan aset ICT, pemasangan dan pengoperasian peralatan dan perisian sama ada dalam bentuk elektronik atau bukan elektronik;

ix. Peralatan Rangkaian

Peralatan rangkaian atau peranti rangkaian komputer berfungsi sebagai pengantara data dalam rangkaian komputer. Peralatan rangkaian termasuklah *switch*, *core switch* dan *firewall*;

x. Media Komunikasi


Semua peralatan berkaitan komunikasi seperti media cetak, media audio, media visual, media audio visual, aplikasi media sosial, internet dan sebagainya; dan

xi. Premis Komputer Dan Komunikasi

Semua kemudahan serta premis yang digunakan untuk menempatkan perkara (i) - (x) di atas.

Setiap perkara di atas perlu diberi perlindungan rapi. Sebarang kebocoran maklumat atau kelemahan perlindungan dianggap sebagai pelanggaran DKICT.

Dasar ini adalah terpakai kepada semua pengguna di Pentadbiran Kerajaan Negeri Sembilan termasuk kakitangan, pembekal dan pakar runding yang mengurus, menyedia, menyelenggara, memproses, mencapai, memuat turun, memuat naik, berkongsi, menyimpan, menggunakan dan melupus aset ICT Kerajaan Negeri Sembilan.

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT Pentadbiran Kerajaan Negeri Sembilan dan perlu dipatuhi adalah seperti berikut:

i. Akses Atas Dasar Perlu Mengetahui


Akses terhadap penggunaan Aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar “perlu mengetahui” sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen Arahan Keselamatan perenggan 53, muka surat 15;

ii. Hak Akses Minimum

Hak akses pengguna hanya diberi pada tahap yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujudkan, menyimpan, mengemas kini, mengubah atau membatalkan sesuatu maklumat. Hak akses perlu dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas;

iii. Akauntabiliti


Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap Aset ICT. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber ICT. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

mampu menyokong kemudahan mengesan atau mengesah bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka.

Akauntabiliti atau tanggungjawab pengguna termasuklah:

- a. menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
- b. memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa;
- c. menentukan maklumat sedia untuk digunakan;
- d. menjaga kerahsiaan kata laluan;
- e. mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
- f. memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
- g. menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

iv. Pengasingan

Tugas mewujudkan, memadam, kemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan dari capaian yang tidak dibenarkan serta melindungi Aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian;

v. Pengauditan


Pengauditan merupakan tindakan untuk mengenalpasti insiden berkaitan keselamatan atau mengenalpasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Dengan itu, Aset ICT seperti komputer, pelayan, *router*, *firewall* dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail*;

vi. Pematuhan

DKICT Pentadbiran Kerajaan Negeri Sembilan hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan ICT;

vii. Pemulihan

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan boleh dilakukan melalui aktiviti penduaan dan mewujudkan pelan pemulihan bencana/ kesinambungan perkhidmatan; dan

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

viii. Saling Bergantungan

Setiap prinsip di atas adalah saling lengkap-melengkapi dan bergantung antara satu sama lain. Dengan itu, tindakan mempelbagaikan pendekatan dalam menyusun dan mencorakkan sebanyak mungkin mekanisme keselamatan adalah perlu bagi menjamin keselamatan yang maksimum.


PENILAIAN RISIKO KESELAMATAN ICT

Pentadbiran Kerajaan Negeri Sembilan hendaklah mengambil kira kewujudan risiko ke atas Aset ICT akibat daripada ancaman dan *vulnerability* yang semakin meningkat hari ini. Justeru itu, Pentadbiran Kerajaan Negeri Sembilan perlu mengambil langkah-langkah proaktif dan bersesuaian untuk menilai tahap risiko Aset ICT supaya pendekatan dan keputusan yang paling berkesan dikenalpasti bagi menyediakan perlindungan dan kawalan ke atas Aset ICT.

Pentadbiran Kerajaan Negeri Sembilan hendaklah melaksanakan penilaian risiko keselamatan ICT secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan ICT. Seterusnya mengambil tindakan susulan dan/atau langkah-langkah bersesuaian untuk mengurangkan

atau mengawal risiko keselamatan ICT berdasarkan penemuan penilaian risiko.

Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat Pentadbiran Kerajaan Negeri Sembilan termasuklah aplikasi, perisian, pelayan, rangkaian dan/atau proses serta prosedur. Penilaian risiko ini hendaklah juga dilaksanakan di premis yang menempatkan sumber-sumber

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

teknologi maklumat termasuklah pusat data, bilik media storan, kemudahan utiliti dan sistem-sistem sokongan lain.

Pentadbiran Kerajaan Negeri Sembilan bertanggungjawab melaksanakan dan menguruskan risiko keselamatan ICT selaras dengan keperluan Surat Pekeliling Am Bilangan 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam dan pemakaian Surat Arahan Ketua Pengarah MAMPU bertarikh 12 Ogos 2015: Pelaksanaan Penilaian Risiko Keselamatan Maklumat Menggunakan MyRAM App.2.0 di agensi Sektor Awam.

Pentadbiran Kerajaan Negeri Sembilan perlu mengenalpasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

- a. mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;
- b. menerima dan/ atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan jabatan;
- c. mengelak dan/atau mencegah risiko dari terjadi dengan mengambil tindakan yang dapat mengelak dan/ atau mencegah berlakunya risiko; dan
- d. memindahkan risiko kepada pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

BIDANG 01 PEMBANGUNAN DAN PENYELENGGARAAN DASAR

0101 Dasar Keselamatan ICT

Objektif:

Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat dan Aset ICT selaras dengan keperluan Kerajaan Negeri Sembilan dan perundangan yang berkaitan.

010101 Pelaksanaan Dasar

Pelaksanaan dasar ini akan dijalankan oleh Setiausaha Kerajaan Negeri dibantu oleh Jawatankuasa Pemandu ICT Kerajaan Negeri Sembilan (JPICNTS) yang terdiri daripada senarai di sub bidang 020109 – Jawatan Kuasa Pemandu ICT Negeri Sembilan (DKICNTS) .


Pelaksanaan dasar ini hendaklah disokong oleh prosedur-prosedur yang lebih terperinci untuk memastikan keberkesanan penyataan dasar.

Setiausaha
Kerajaan Negeri
Sembilan,
CIO
dan
ICTSO


010102 Penyebaran Dasar

Dasar ini perlu disebarkan kepada semua pengguna ICT Pentadbiran Kerajaan Negeri Sembilan termasuk


ICTSO

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

kakitangan, pembekal, pakar runding dan lain-lain.	
010103 Penyelenggaraan Dasar	
<p>DKICT Pentadbiran Kerajaan Negeri Sembilan adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa termasuk kawalan keselamatan, prosedur dan proses selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan, dasar Kerajaan dan kepentingan sosial.</p> <p>Berikut adalah prosedur yang berhubung dengan penyelenggaraan DKICT Pentadbiran Kerajaan Negeri Sembilan:</p> <ol style="list-style-type: none"> kenal pasti dan tentukan perubahan yang diperlukan; kemuka cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan mesyuarat Jawatankuasa Pemandu ICT Kerajaan Negeri Sembilan (JPICTNS); maklum kepada semua pengguna ICT perubahan yang telah dipersetujui oleh mesyuarat Jawatankuasa Pemandu ICT Kerajaan Negeri Sembilan (JPICTNS); dan 	<p>JPICTNS dan ICTSO</p>

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

iv. dasar ini hendaklah dikaji semula sekurang-kurangnya sekali dalam tempoh tiga (3) tahun atau mengikut keperluan semasa untuk memastikan dasar sentiasa relevan dan efisien.	
010104 Pematuhan Dasar	
DKICT Pentadbiran Kerajaan Negeri Sembilan adalah terpakai kepada semua pengguna ICT Pentadbiran Kerajaan Negeri Sembilan dan tiada pengecualian diberikan.	Semua

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

BIDANG 02 - ORGANISASI KESELAMATAN

0201 Struktur Organisasi Dalaman

Objektif:


Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif DKICT Pentadbiran Kerajaan Negeri Sembilan.

020101 Setiausaha Kerajaan Negeri Sembilan


Setiausaha Kerajaan Negeri Sembilan berperanan dan bertanggungjawab dalam perkara-perkara berikut:

- i. menetapkan hala tuju dan strategi untuk pelaksanaan keselamatan ICT bagi semua Jabatan/ Agensi di bawah pentadbiran Kerajaan Negeri Sembilan;
- ii. memastikan semua pengguna memahami peruntukan-peruntukan di bawah DKICT Pentadbiran Kerajaan Negeri Sembilan;
- iii. memastikan semua pengguna mematuhi DKICT Pentadbiran Kerajaan Negeri Sembilan;


Setiausaha
Kerajaan Negeri
Sembilan

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


<ul style="list-style-type: none"> iv. memastikan semua keperluan organisasi (sumber kewangan, sumber manusia dan perlindungan keselamatan) adalah mencukupi; v. memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam DKICT Pentadbiran Kerajaan Negeri Sembilan; dan vi. menguruskan mesyuarat Jawatankuasa Pemandu ICT Kerajaan Negeri Sembilan (JPICTNS). 	
020102 Ketua Pegawai Maklumat (CIO)	
<p>Ketua Pegawai Maklumat atau <i>Chief Information Officer</i> (CIO) Pentadbiran Kerajaan Negeri Sembilan ialah Timbalan Setiausaha Kerajaan Negeri (Pengurusan), Ketua Jabatan dan Pegawai yang dilantik. Peranan dan tanggungjawab CIO adalah seperti berikut:</p> <ul style="list-style-type: none"> i. membantu Setiausaha Kerajaan Negeri Sembilan dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; ii. menentukan keperluan keselamatan ICT; 	CIO

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


<ul style="list-style-type: none"> iii. menguatkuasakan DKICT Pentadbiran Kerajaan Negeri Sembilan; iv. memperkasakan tadbir urus keselamatan ICT Jabatan/ Agensi; v. merancang pelan latihan dan program kesedaran keselamatan ICT seperti penyediaan/ pengemaskinian DKICT Pentadbiran Kerajaan Negeri Sembilan serta pengurusan risiko dan pengauditan; dan vi. bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT Pentadbiran Kerajaan Negeri Sembilan. 	
020103 Pegawai Keselamatan ICT (ICTSO)	
<p>Pegawai Keselamatan ICT (ICTSO) bagi Pentadbiran Kerajaan Negeri Sembilan ialah Ketua Jabatan ICT di Jabatan/Agensi masing-masing. Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut :</p> <ul style="list-style-type: none"> i. mengurus, menyedia dan melaksanakan keseluruhan program-program keselamatan ICT; ii. membantu menguatkuasakan pelaksanaan DKICT; 	ICTSO

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


<ul style="list-style-type: none"> iii. memberi penerangan dan pendedahan berkenaan DKICT kepada semua pengguna; iv. mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan DKICT; v. menjalankan pengurusan risiko dan keselamatan ICT; vi. menjalankan audit, kajian semula, merumus tindak balas pengurusan Pentadbiran Kerajaan Negeri Sembilan berdasarkan hasil penemuan dan menyediakan laporan mengenainya; vii. memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; viii. melaporkan insiden keselamatan ICT kepada Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan Negeri Sembilan (CERTNS), CIO dan kepada pihak NACSA sekiranya perlu; ix. bekerjasama dengan semua pihak yang berkaitan dalam mengenalpasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah- 	
--	--

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


<p>langkah baik pulih dengan segera;</p> <p>x. menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan; dan</p> <p>xi. bertanggungjawab sebagai Koordinator Pengurusan Pelan Pemulihan Bencana/ <i>Disaster Recovery Plan</i> (DRP) Pentadbiran Kerajaan Negeri Sembilan.</p>	
020104 Pegawai Keselamatan Jabatan (PKJ)	
<p>Pegawai Keselamatan Jabatan (PKJ) merupakan pegawai yang bertanggungjawab sepenuhnya mengenai keselamatan dalam Jabatannya seperti yang ditetapkan di Para 16, Buku Arah Keselamatan Kerajaan. Peranan dan tanggungjawab PKJ adalah seperti berikut:</p> <p>i. bertanggungjawab ke atas semua aspek keselamatan dokumen dan maklumat rasmi Jabatan/Agensi, bangunan dan harta benda Kerajaan daripada sebarang ancaman, kecurian, kebakaran dan sebagainya dengan mengambilkira</p>	<p>Pegawai Keselamatan Jabatan</p>

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

<p>langkah-langkah melindungi selaras dengan peraturan- peraturan yang ditetapkan oleh Kerajaan;</p> <p>ii. mengemukakan perakuan-perakuan kepada Setiausaha Kerajaan Negeri/Ketua Jabatan cadangan-cadangan untuk meningkatkan langkah-langkah Keselamatan Perlindungan dari semasa ke semasa mengikut kesesuaian;</p> <p>iii. mewakili Jabatan/Agensi Kerajaan dalam menghadiri mesyuarat mengenai keselamatan dari semasa ke semasa dan jika diperlukan hendaklah membentangkan laporan keselamatan Agensi/ Jabatan serta isu-isu yang tidak dapat diselesaikan di peringkat Jabatan/Agensi;</p> <p>iv. mengadakan pemeriksaan dari semasa ke semasa ke atas bangunan, sistem pendawaian elektrik, bilik komputer, bilik dokumen dan peralatan, kawasan pejabat dan semua perkara di bawah tanggungjawabnya bagi memastikan dalam keadaan yang selamat dan tidak terdedah kepada ancaman dan risiko;</p> <p>v. menganjurkan kursus dan taklimat kesedaran Keselamatan Perlindungan; dan</p>	
--	--

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


vi. melaksanakan tugas-tugas lain yang ditetapkan dalam peraturan- peraturan keselamatan Kerajaan yang sedang berkuatkuasa dan yang dipinda dari semasa ke semasa.	
020105 Pengurus ICT	
<p>Pengurus ICT merupakan pegawai yang bertanggungjawab menguruskan keselamatan ICT meliputi aplikasi, operasi dan rangkaian di bawah kawalannya. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut:</p> <ul style="list-style-type: none"> i. mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan Pentadbiran Kerajaan Negeri Sembilan; ii. melaksanakan sistem kawalan capaian pengguna ke atas aset ICT; iii. melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; iv. menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT; v. memastikan semua kakitangan, perunding, kontraktor dan pembekal yang terlibat dengan Jabatan/Agensi mematuhi dasar, piawaian dan garis 	Pengurus ICT

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


<p>panduan keselamatan ICT dan seterusnya melaporkan sebarang insiden berkaitan keselamatan ICT;</p> <p>vi. melaksanakan keperluan DKICT dalam operasi semasa seperti berikut:</p> <ul style="list-style-type: none"> • pelaksanaan sistem atau aplikasi baru sama ada dibangunkan secara dalaman atau luaran; • pembelian atau peningkatan perisian dan sistem komputer; • perolehan teknologi dan perkhidmatan komunikasi; dan • memastikan pihak luaran melaksanakan peranan seperti di sub bidang 0202 – Pihak Luaran. <p>vii. membangunkan garis panduan, prosedur dan tatacara untuk aplikasi khusus (sekiranya perlu); dan</p> <p>viii. membangun, mengkaji semula dan mengemas kini pelan kontingensi keselamatan ICT.</p>	
--	--

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


020106 Pentadbir Sistem ICT	
<p>Pentadbir Sistem ICT bagi Pentadbiran Kerajaan Negeri Sembilan terdiri daripada:</p> <ul style="list-style-type: none"> i. Pentadbir Rangkaian Dan Keselamatan; ii. Pentadbir Pangkalan Data; iii. Pentadbir Portal/Laman Web (Webmaster); iv. Pentadbir Pusat Data/<i>Bilik Server</i>; v. Pentadbir Sistem Aplikasi; dan vi. Pentadbir E-Mel. 	Pentadbir Sistem ICT
020106A Pentadbir Rangkaian Dan Keselamatan	
<p>Peranan dan tanggungjawab Pentadbir Rangkaian dan Keselamatan adalah seperti berikut:</p> <ul style="list-style-type: none"> i. memastikan rangkaian setempat (LAN) dan rangkaian luas (WAN) di Pentadbiran Kerajaan Negeri Sembilan beroperasi sepanjang masa; ii. memastikan semua peralatan dan perisian rangkaian 	Pentadbir Rangkaian Dan Keselamatan

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


<p>dan keselamatan diselenggarakan dengan sempurna;</p> <p>iii. merancang peningkatan infrastruktur, ciri-ciri keselamatan dan prestasi rangkaian sedia ada;</p> <p>iv. mengesan dan mengambil tindakan pembaikan segera ke atas rangkaian yang tidak stabil;</p> <p>v. memantau penggunaan rangkaian dan melaporkan kepada ICTSO sekiranya berlaku penyalahgunaan sumber rangkaian;</p> <p>vi. memastikan laluan trafik keluar dan masuk diuruskan secara berpusat dan tidak membenarkan sambungan ke rangkaian Pentadbiran Kerajaan Negeri Sembilan secara tidak sah seperti melalui peralatan modem dan <i>dial-up</i>;</p> <p>vii. menyediakan zon khas rangkaian untuk tujuan pengujian peralatan dan perisian rangkaian; dan</p> <p>viii. melaksanakan penilaian tahap keselamatan sistem rangkaian dan sistem ICT (<i>Security Posture Assessment</i> (SPA)) serta penilaian risiko keselamatan maklumat.</p>	
--	--

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

020106B Pentadbir Pangkalan Data	
<p>Peranan dan tanggungjawab Pentadbir Pangkalan Data adalah seperti berikut:</p> <ul style="list-style-type: none"> i. melaksanakan polisi pengguna pangkalan data berdasarkan kepada prinsip-prinsip DKICT; ii. melaksanakan pemantauan dan penyelenggaraan yang berterusan ke atas pangkalan data; iii. memastikan aktiviti pentadbiran pangkalan data seperti kawalan capaian dan proses pengemaskinian data dilaksanakan dengan teratur; dan iv. melaporkan sebarang insiden pelanggaran dasar keselamatan pangkalan data kepada ICTSO. 	Pentadbir Pangkalan Data
020106C Pentadbir Laman Web (Webmaster)	
<p>Peranan dan tanggungjawab Pentadbir Laman Web (<i>Webmaster</i>) adalah seperti berikut:</p> <ul style="list-style-type: none"> i. menerima kandungan laman web yang telah disahkan kesahihan dan terkini daripada sumber yang sah; 	Pentadbir Laman Web (<i>Webmaster</i>)

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


<ul style="list-style-type: none"> ii. memantau dan menganalisis log untuk mengesan sebarang capaian yang tidak sah atau cubaan menggodam, mencero boh dan mengubahsuai muka laman; iii. memastikan reka bentuk web dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi; iv. melaksanakan <i>housekeeping</i> keselamatan terhadap sistem pengoperasian dan perisian-perisian lain di <i>web server</i>; dan v. melaporkan sebarang pelanggaran keselamatan laman web kepada ICTSO. 	
020106D Pentadbir Pusat Data/Bilik Server	
<p>Peranan dan tanggungjawab Pentadbir Pusat Data/Bilik <i>Server</i> adalah seperti berikut:</p> <ul style="list-style-type: none"> i. memastikan persekitaran fizikal dan keselamatan pusat data dalam keadaan baik dan selamat; ii. memastikan keselamatan data dan sistem aplikasi di dalam Pusat Data/Bilik <i>Server</i>; iii. menjadual dan melaksanakan proses <i>backup</i> dan <i>restoration</i> ke atas pangkalan data dan sistem secara 	<p>Pentadbir Pusat Data</p>

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

berkala; dan	
iv. melaporkan sebarang pelanggaran keselamatan Pusat Data/Bilik Server kepada ICTSO.	

020106E Pentadbir Sistem Aplikasi


<p>Peranan dan tanggungjawab Pentadbir Sistem Aplikasi adalah seperti berikut:</p> <ul style="list-style-type: none"> i. mengkaji cadangan pembangunan atau penyelarasan sistem; ii. membuat kajian semula serta menambahbaik sistem sedia ada; iii. membuat pemantauan dan penyelenggaraan terhadap sistem; iv. bertanggungjawab dalam aspek-aspek pelaksanaan keseluruhan sistem; v. menyediakan dokumentasi sistem dan manual pengguna; vi. memastikan kelancaran operasi sistem aplikasi supaya perkhidmatan yang disediakan tidak terjejas; 	Pentadbir Sistem Aplikasi
--	---------------------------

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


<p>vii. memastikan kod-kod program sistem aplikasi adalah selamat daripada penggodam sebelum sistem tersebut diaktifkan penggunaannya;</p> <p>viii. mematuhi dan melaksanakan prinsip-prinsip DKICT dalam pewujudan akaun pengguna ke atas setiap sistem aplikasi; dan</p> <p>ix. melaporkan kepada ICTSO jika berlakunya insiden keselamatan ke atas sistem aplikasi di bawah seliaannya.</p>	
020106F Pentadbir E-mel	
<p>Peranan dan tanggungjawab Pentadbir E-mel adalah seperti berikut:</p> <p>i. menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan. Pembatalan akaun (pengguna yang berhenti, bertukar dan melanggar dasar dan polisi) perlulah dilakukan dengan segera atas tujuan keselamatan maklumat;</p> <p>ii. Pentadbir E-mel boleh membekukan akaun pengguna jika perlu semasa pengguna bercuti panjang, berkursus atau menghadapi tindakan tatatertib;</p>	Pentadbir E-mel

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

<ul style="list-style-type: none"> iii. memastikan kemudahan membuat capaian E-mel melalui pelbagai peralatan ICT dan alat komunikasi; iv. memastikan pengguna e-mel Pentadbiran Kerajaan Negeri Sembilan berkemahiran menggunakan e-mel melalui penyediaan dokumen Polisi Penggunaan E-mel Pentadbiran Kerajaan Negeri Sembilan serta pelaksanaan kursus Pembudayaan ICT (Penggunaan E-mel) secara berterusan; dan v. melaporkan sebarang pelanggaran penggunaan perkhidmatan e-mel kepada ICTSO. 	
020107 Pegawai Aset	
<p>Pegawai Aset adalah pegawai yang telah dilantik oleh Jawatankuasa Pengurusan Aset (JKPAK) / Ketua Jabatan. Peranan dan tanggungjawab Pegawai Aset adalah seperti yang terkandung di dalam 1 Pekeliling Perbendaharaan : Tatacara Pengurusan Aset Alih Kerajaan :</p> <ul style="list-style-type: none"> i. bertanggungjawab terhadap kesiapsediaan, selenggaraan dan keselamatan aset untuk kegunaan harian; dan ii. bertanggungjawab memantau perkakasan ICT yang diagihkan kepada pengguna. 	<p>Pegawai Aset</p>

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

020108 Pengguna	
<p>Pengguna mempunyai peranan dan tanggungjawab seperti berikut:</p> <ul style="list-style-type: none"> i. membaca, memahami dan mematuhi DKICT Pentadbiran Kerajaan Negeri Sembilan; ii. mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; iii. menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat; iv. melaksanakan prinsip-prinsip DKICT Pentadbiran Kerajaan Negeri Sembilan dan menjaga kerahsiaan maklumat Pentadbiran Kerajaan Negeri Sembilan; v. melaksanakan langkah-langkah perlindungan seperti berikut: <ul style="list-style-type: none"> a. menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b. memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; 	Pengguna

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


<ul style="list-style-type: none"> c. menjaga kerahsiaan kata laluan; d. mematuhi standard, prosedur, langkah dan garis panduan keselamatan ICT yang ditetapkan; e. melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan f. menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum. <ul style="list-style-type: none"> vi. melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; vii. menghadiri program-program kesedaran mengenai keselamatan ICT; dan viii. mengawal aktiviti penggunaan media sosial seperti di bawah: <ul style="list-style-type: none"> a. mengelakkan ketirisan maklumat; b. tidak memberi atau mendedahkan sebarang 	
--	--

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


<p>komen, pernyataan atau isu yang menyentuh perkara-perkara yang boleh menjejaskan imej dan dasar kerajaan;</p> <p>c. tidak menyebarkan maklumat yang berbentuk fitnah, hasutan dan lucah atau cuba memprovokasikan sesuatu isu yang menyalahi peraturan dan undang-undang atau perkara yang menyentuh sensitiviti individu atau kumpulan tertentu; dan</p> <p>d. tidak menggunakan saluran media sosial hingga mengganggu fokus dalam urusan kerja.</p> <p>ix. menandatangani Surat Akuan Pematuhan DKICT Pentadbiran Kerajaan Negeri Sembilan seperti di Lampiran 1.</p>	
020109 Jawatankuasa Pemandu ICT Negeri Sembilan (JPICTNS)	
<p>Jawatankuasa Pemandu ICT Negeri Sembilan (JPICTNS) merupakan jawatankuasa yang bertanggungjawab dalam keselamatan ICT dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan ICT Pentadbiran Kerajaan Negeri Sembilan. Keanggotaan JPICTNS adalah seperti berikut:</p>	JPICTNS

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


<p><u>Pengerusi:</u></p> <p>Setiausaha Kerajaan Negeri</p> <p><u>Ahli Tetap:</u></p> <ol style="list-style-type: none"> 1. Pegawai Kewangan Negeri; 2. Timbalan Setiausaha Kerajaan Negeri (Pembangunan); 3. Timbalan Setiausaha Kerajaan Negeri (Pengurusan); 4. Pengarah, Unit Pengurusan Teknologi Maklumat; 5. Timbalan Pengarah, Unit Pengurusan Teknologi Maklumat; 6. Perunding ICT, MAMPU; 7. Perunding ICT, ICU, JPM; 8. Ketua Jabatan/Agensi Teknikal : <ul style="list-style-type: none"> • Pejabat Tanah dan Galian Negeri Sembilan; • Jabatan Kerja Raya Negeri Sembilan; • PlanMalaysia@Negeri Sembilan; • Jabatan Pengairan dan Saliran Negeri Sembilan; dan • Pejabat Pembangunan Negeri, Negeri Sembilan. 9. Ketua – Ketua Bahagian PSUKNS : <ul style="list-style-type: none"> • Unit Pembangunan Ekonomi Negeri; • Unit Kerajaan Tempatan; • Unit Perumahan; • Bahagian Pembangunan Sumber Manusia; • Unit Korporat, Inovasi dan Kualiti; dan 	
---	--

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

<ul style="list-style-type: none"> • Unit Audit Dalam. <p>10. Pihak Berkuasa Tempatan ; dan</p> <ul style="list-style-type: none"> • Majlis Perbandaran Seremban; • Majlis Perbandaran Nilai; dan • Majlis Perbandaran Port Dickson. <p>11. Semua Pegawai ICT, UPTM Gred 44 dan ke atas.</p> <p><u>Ahli Bukan Tetap (Panel Jemputan):</u></p> <p>Ahli Jawatankuasa Bukan Tetap (Panel Jemputan) boleh dilantik mengikut kesesuaian isu atau permasalahan yang dibincangkan mengikut agenda mesyuarat. Wakil Jabatan/ Agensi yang dijemput hendaklah memainkan peranan sebagai pakar rujuk/penasihat dalam bidang berkaitan.</p> <p><u>Urus Setia:</u></p> <p>Seksyen Multimedia, Korporat dan Koordinasi ICT (MKK), Unit Pengurusan Teknologi Maklumat (UPTM).</p> <p>Bidang kuasa JPICTNS adalah seperti berikut:</p> <ul style="list-style-type: none"> i. menetapkan arah tuju dan strategi untuk pelaksanaan ICT jabatan/agensi pentadbiran Kerajaan Negeri Sembilan; ii. merancang, mengenalpasti dan mencadangkan sumber seperti kepakaran, tenaga kerja dan kewangan yang diperlukan bagi melaksanakan arah 	
--	--

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


<p>tuju/strategi ICT jabatan/agensi pentadbiran Kerajaan Negeri;</p> <p>iii. merancang dan menyelaraskan pelaksanaan program/projek ICT jabatan/agensi pentadbiran Kerajaan Negeri supaya selaras dengan Pelan Strategik ICT Jabatan/Agensi pentadbiran Kerajaan Negeri;</p> <p>iv. menyelaraskan dan menyeragamkan pelaksanaan ICT antara Jabatan/Agensi pentadbiran Kerajaan Negeri dengan Pelan Strategik ICT Sektor Awam;</p> <p>v. mempromosi dan menggalakkan perkongsian pintar projek-projek ICT antara semua Jabatan/Agensi Pentadbiran Kerajaan Negeri;</p> <p>vi. merancang dan menentukan langkah-langkah keselamatan ICT;</p> <p>vii. memantau perkembangan program ICT Jabatan/Agensi pentadbiran Kerajaan Negeri serta memahami keperluan, masalah dan isu-isu yang dihadapi dalam pelaksanaan ICT;</p> <p>viii. meluluskan perolehan ICT bagi Jabatan/Agensi pentadbiran Kerajaan Negeri berdasarkan keperluan sebenar dengan perbelanjaan yang</p>	
---	--

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


<p>berhemah serta mematuhi pekeliling/peraturan semasa yang berkaitan;</p> <p>ix. menyelaraskan dan mengemukakan laporan perolehan ICT Jabatan/Agensi di bawah pentadbiran Kerajaan Negeri kepada Urus Setia JTICT menikut tempoh yang telah ditetapkan; dan</p> <p>x. menyelaraskan pelaksanaan program-program merapatkan jurang digital peringkat negeri.</p>	
020110 Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan Negeri Sembilan (CERTNS)	
<p>Pasukan CERTNS ditubuhkan bagi membantu mengendalikan insiden keselamatan ICT, mengawasi dan memberi nasihat berkaitan keselamatan ICT kepada agensi-agensi di bawah kawalannya.</p> <p>Keanggotaan CERTNS adalah seperti berikut:</p> <p><u>Pengarah :</u> Pengarah Unit Pengurusan Teknologi Maklumat (UPTM)</p>	<p>CERTNS</p>

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


<p><u>Pengurus :</u></p> <p>Penolong Pengarah (Kanan) (Operasi dan Rangkaian), Unit Pengurusan Teknologi Maklumat (UPTM)</p> <p><u>Ahli Tetap:</u></p> <ol style="list-style-type: none"> 1. Timbalan Pengarah, UPTM 2. Penolong Pengarah Kanan (Seksyen Pembangunan dan Penyelenggaraan Sistem), UPTM 3. Penolong Pengarah Kanan (Seksyen Multimedia, Korporat & Koordinasi ICT), UPTM 4. Penolong Pengarah (Seksyen Keselamatan & Pangkalan Data), UPTM 5. Penolong Pengarah (Seksyen Operasi & Sokongan Teknikal), UPTM 6. Penolong Pengarah (Seksyen Perancangan Infrastruktur & Rangkaian ICT), UPTM 7. Penolong Pegawai Teknologi Maklumat (Seksyen Keselamatan & Pangkalan Data), UPTM 8. Penolong Pegawai Teknologi Maklumat (Seksyen Operasi & Sokongan Teknikal), UPTM 9. Penolong Pegawai Teknologi Maklumat (Seksyen Perancangan Infrastruktur & Rangkaian ICT), UPTM 10. Pegawai Teknologi Maklumat, Pejabat Tanah dan Galian Negeri Sembilan; dan 11. Pegawai Teknologi Maklumat, Pejabat Kewangan Negeri Sembilan. 	
--	--

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

<p><u>Ahli Dilantik:</u></p> <ol style="list-style-type: none"> 1. Unit Pengurusan Teknologi Maklumat; 2. Wakil Pihak Berkuasa Tempatan; 3. Wakil Pejabat Tanah dan Daerah; dan 4. Wakil Jabatan/Agensi <p>Peranan dan tanggungjawab CERTNS adalah seperti berikut:</p> <ol style="list-style-type: none"> i. menerima dan mengesan aduan keselamatan ICT serta menilai tahap dan jenis insiden; ii. merekodkan dan menjalankan siasatan awal insiden yang diterima; iii. menangani tindak balas insiden keselamatan ICT dan mengambil tindakan baik pulih minimum; iv. menasihati agensi di bawah Pentadbiran Kerajaan Negeri Sembilan supaya mengambil tindakan pemulihan dan pengukuhan; dan v. menyebarkan makluman berkaitan pengukuhan keselamatan ICT kepada Pentadbiran Kerajaan Negeri Sembilan. 	
---	--

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


0202 Pihak Luaran	
<p>Objektif:</p> <p>Menjamin keselamatan semua Aset ICT yang digunakan oleh pihak luaran. Pihak luaran adalah terdiri daripada pembekal, pakar runding dan pihak-pihak lain yang terlibat dalam penggunaan atau capaian kepada aset dan perkhidmatan ICT Jabatan.</p>	
020201 Keperluan Keselamatan Kontrak dengan Pihak Luaran	
<p>Ini bertujuan memastikan penggunaan Aset ICT, penggunaan maklumat dan kemudahan proses maklumat oleh pihak luaran dikawal. Perkara yang perlu dipatuhi termasuk perkara berikut:</p> <ul style="list-style-type: none"> i. mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; ii. mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak luaran; iii. akses kepada Aset ICT Pentadbiran Kerajaan Negeri Sembilan perlu berlandaskan kepada prosedur-prosedur keselamatan yang berkaitan; 	<p>CIO, ICTSO, Pengurus ICT, Pentadbir Sistem ICT dan Pihak Luaran</p>

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

<p>iv. memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak luaran. Perkara-perkara berikut hendaklah dimasukkan dalam perjanjian yang dimeterai.</p> <p>a. DKICT Pentadbiran Kerajaan Negeri Sembilan;</p> <p>b. <i>Non-Disclosure Agreement</i> (NDA);</p> <p>c. Arahan Teknologi Maklumat 2007 (<i>IT Instructions</i>);</p> <p>d. Perakuan Akta Rahsia Rasmi 1972; dan</p> <p>e. Tapisan keselamatan.</p> <p>v. membaca, memahami dan menandatangani Surat Akuan Pematuhan DKICT Pentadbiran Kerajaan Negeri Sembilan seperti di Lampiran 1, <i>Non-Disclosure Agreement</i> (NDA) seperti di Lampiran 2 dan Perakuan Akta Rahsia Rasmi 1972 seperti di Lampiran 3.</p>	
---	--

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


BIDANG 03 PENGURUSAN ASET	
0301 Akauntabiliti Aset	
<p>Objektif:</p> <p>Memberi dan menyokong perlindungan yang sepatutnya ke atas semua Aset ICT pelbagai Jabatan/Agensi di bawah Pentadbiran Kerajaan Negeri Sembilan.</p>	
030101 Inventori Aset ICT	
<p>Ini bertujuan memastikan semua Aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Perkara yang perlu dipatuhi adalah seperti berikut:</p> <ul style="list-style-type: none"> i. memastikan semua aset ICT dikenal pasti, dikelas, didokumen, diselenggara dan dilupuskan. Maklumat aset direkod dan dikemaskini dalam Sistem Pengurusan Aset, Kad Daftar Harta Modal dan Aset Bernilai Rendah sebagaimana mengikut Pekeliling Perbendaharaan AM 2.1 Tahun 2013 : Tatacara Pengurusan Aset Alih Kerajaan; ii. memastikan semua Aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; 	<p>Pegawai Aset dan Pengguna</p>

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


<ul style="list-style-type: none"> iii. memastikan semua pengguna mengesahkan penempatan Aset ICT yang ditempatkan di semua Jabatan/Agensi di bawah Pentadbiran Kerajaan Negeri Sembilan; iv. peraturan bagi pengendalian Aset ICT hendaklah dikenal pasti, didokumen dan dilaksanakan oleh Pegawai Aset; v. setiap pengguna adalah bertanggungjawab ke atas semua Aset ICT di bawah kawalannya termasuk Aset ICT yang dipinjamkan; vi. pengguna yang dibekalkan dengan Aset ICT bertanggungjawab melaporkan kerosakan kepada Pegawai Aset; dan vii. Ketua Jabatan atau pegawai bertanggungjawab hendaklah membuat laporan polis dengan segera, tidak lewat dari 24 jam selepas berlaku kehilangan. 	
0302 Pengelasan dan Pengendalian Maklumat	
<p>Objektif:</p> <p>Memastikan setiap maklumat atau Aset ICT diberikan tahap perlindungan yang bersesuaian.</p>	

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

030201 Pengelasan Maklumat	
<p>Maklumat hendaklah dikelaskan atau dilabelkan sewajarnya oleh pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan.</p> <p>Setiap maklumat yang dikelaskan hendaklah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut:</p> <ul style="list-style-type: none"> i. Rahsia Besar; ii. Rahsia; iii. Sulit; atau iv. Terhad. 	Pengguna
030202 Pengendalian Maklumat	
<p>Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampaikan, menukar dan memusnahkan hendaklah mengambilkira langkah-langkah keselamatan berikut:</p> <ul style="list-style-type: none"> i. menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; 	Pentadbir Sistem ICT dan Pengguna

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

<ul style="list-style-type: none"> iii. menentukan maklumat sedia untuk digunakan; iv. menjaga kerahsiaan kata laluan; v. mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; vi. memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan vii. menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum. 	
---	--

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

BIDANG 04 KESELAMATAN SUMBER MANUSIA

0401 Keselamatan Sumber Manusia Dalam Tugas Harian

Objektif:

Memastikan semua sumber manusia yang terlibat di bawah Pentadbiran Kerajaan Negeri Sembilan dan pihak-pihak yang berkepentingan memahami tanggungjawab dan peranan, meningkatkan pengetahuan dalam keselamatan Aset ICT serta mematuhi terma dan syarat perkhidmatan dan peraturan semasa yang berkuat kuasa.

040101 Sebelum Perkhidmatan

Memastikan semua pengguna yang berkepentingan memahami tanggungjawab masing-masing ke atas keselamatan aset ICT bagi meminimumkan risiko seperti kesilapan, kecuaiian, penipuan dan penyalahgunaan aset ICT.


Pentadbir
Sistem ICT
dan
Pengguna

Perkara yang perlu dipatuhi adalah seperti berikut:

- i. menyatakan dengan lengkap serta jelas peranan dan tanggungjawab semua pengguna di bawah Pentadbiran Kerajaan Negeri Sembilan serta pihak luaran yang terlibat dalam menjamin keselamatan Aset ICT sebelum, semasa dan selepas perkhidmatan;

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


<ul style="list-style-type: none"> ii. menjalankan tapisan keselamatan untuk semua pengguna di bawah Pentadbiran Kerajaan Negeri Sembilan serta pihak luaran yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; iii. memastikan pihak luaran menandatangani Surat Akuan Pematuhan DKICT Pentadbiran Kerajaan Negeri Sembilan, <i>Non-Disclosure Agreement</i> (NDA), Arahan Teknologi Maklumat 2007 (<i>IT Instructions</i>), Perakuan Akta Rahsia Rasmi 1972 dan Tapisan Keselamatan; dan iv. mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan. 	
040102 Dalam Perkhidmatan	
<p>Memastikan semua pengguna yang berkepentingan sedar akan ancaman keselamatan maklumat, peranan dan tanggungjawab masing-masing untuk menyokong DKICT Pentadbiran Kerajaan Negeri Sembilan dan meminimumkan risiko kesilapan, kecuai, kecurian, penipuan dan penyalahgunaan aset ICT.</p>	<p>Pentadbir Sistem ICT dan Pengguna</p>

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


<p>Perkara-perkara yang perlu dipatuhi termasuk:</p> <ul style="list-style-type: none"> i. memastikan semua pengguna di bawah Pentadbiran Kerajaan Negeri Sembilan serta pihak luaran yang berkepentingan mengurus keselamatan Aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh Pentadbiran Kerajaan Negeri Sembilan atau Jabatan/Agensi yang berkenaan; ii. memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan Aset ICT diberi kepada pengguna ICT di bawah Pentadbiran Kerajaan Negeri Sembilan secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak luaran yang berkepentingan dari semasa ke semasa; iii. memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas pegawai dan kakitangan di bawah Pentadbiran Kerajaan Negeri Sembilan serta pihak luaran yang berkepentingan sekiranya berlaku pelanggaran dengan perundangan dan peraturan ditetapkan oleh Pentadbiran Kerajaan Negeri Sembilan atau Jabatan/Agensi yang berkenaan; dan 	
--	--

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


<p>iv. memantapkan pengetahuan berkaitan dengan penggunaan Aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT. Sebarang kursus dan latihan teknikal yang diperlukan, pengguna boleh merujuk kepada Bahagian Pengurusan Sumber Manusia, Pejabat Setiausaha Kerajaan Negeri Sembilan atau Jabatan/Agensi yang berkenaan.</p>	
040103 Bertukar Atau Tamat Perkhidmatan	
<p>Memastikan pertukaran, tamat perkhidmatan atau perubahan bidang tugas semua pengguna yang berkepentingan diuruskan dengan teratur.</p> <p>Perkara-perkara yang perlu dipatuhi termasuk:</p> <ul style="list-style-type: none"> i. memastikan semua Aset ICT dikembalikan kepada pegawai yang dipertanggungjawabkan di bawah Jabatan/Agensi yang berkenaan mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan ii. membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh Jabatan/Agensi yang berkenaan. 	<p>Pentadbir Sistem ICT, Pegawai Aset dan Pengguna</p>

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


040104 Program Kesedaran Keselamatan ICT	
Semua pengguna yang berkepentingan perlu diberikan program kesedaran mengenai keselamatan ICT secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka.	ICTSO dan Pengurus ICT

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


BIDANG 05 KESELAMATAN FIZIKAL DAN PERSEKITARAN	
0501 Keselamatan Kawasan	
<p>Objektif:</p> <p>Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta capaian yang tidak dibenarkan.</p>	
050101 Kawalan Kawasan	
<p>Ini bertujuan untuk menghalang capaian, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat jabatan. Perkara-perkara yang perlu dipatuhi termasuk:</p> <ul style="list-style-type: none"> i. Kawasan keselamatan fizikal hendaklah dikenalpasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko. Contoh: Pusat Data/Bilik <i>Server</i>; ii. menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; 	<p>CIO, ICTSO, Pegawai Aset dan Pegawai Keselamatan Jabatan (PKJ)</p>

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


<ul style="list-style-type: none"> iii. memasang alat penggera atau kamera litar tertutup (CCTV); iv. menghadkan laluan keluar masuk dengan penggunaan sistem imbasan biometrik; v. mewujudkan kaunter perkhidmatan dan kawalan; vi. menyediakan tempat atau bilik khas pelawat; vii. melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; viii. merekabentuk dan melaksanakan keselamatan fizikal di dalam bangunan dan kawasan yang berisiko; ix. merekabentuk dan melaksanakan perlindungan fizikal daripada bencana seperti kebakaran, banjir, letupan dan sebagainya; x. menyediakan garis panduan untuk pegawai dan kakitangan yang bekerja di dalam kawasan larangan; dan xi. memastikan kawalan keluar masuk dikawasan penghantaran, pemunggahan dan lain-lain tempat. 	
--	--

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

050102 Kawalan Masuk Fizikal	
<p>Perkara-perkara yang perlu dipatuhi termasuk:</p> <ul style="list-style-type: none"> i. setiap pegawai dan kakitangan di bawah Pentadbiran Kerajaan Negeri Sembilan hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; ii. semua pas keselamatan hendaklah diserahkan balik kepada ketua jabatan apabila pegawai dan kakitangan bertukar, berhenti atau bersara; iii. setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di pintu kawalan utama atau jabatan terlibat. Pas ini hendaklah dikembalikan semula selepas tamat lawatan; dan iv. kehilangan pas hendaklah dilaporkan dengan segera. 	<p>Pentadbir Sistem ICT</p>
050103 Kawasan Larangan	
<p>Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pegawai-pegawai tertentu sahaja. Ini dilaksanakan untuk melindungi Aset ICT yang terdapat di dalam kawasan tersebut.</p>	<p>Pegawai Keselamatan Jabatan (PKJ), Pengurus ICT,</p>

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

<p>Kawasan larangan adalah seperti berikut :</p> <ul style="list-style-type: none"> i. Bilik YAB Menteri Besar; ii. Bilik YB SUK; iii. Bilik EXCO; iv. Bilik Timbalan SUK; v. Dewan Undangan Negeri; vi. Bilik Pegawai Daerah/Yang Dipertua; vii. Bilik Ketua Jabatan/Bahagian/Unit; viii. Pusat Data/ Bilik Server; ix. Bilik peralatan keselamatan; x. <i>Disaster Recovery Centre</i> (DRC); dan xi. Kawasan yang berisiko <p>Akses kepada kawasan larangan hanyalah kepada pegawai yang dibenarkan sahaja. Kawasan ini mestilah dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam. Kawalan keselamatan ke atas premis tersebut adalah seperti berikut:</p> <ul style="list-style-type: none"> i. sumber data atau pelayan, peralatan komunikasi dan storan perlu ditempatkan di pusat data, bilik server atau bilik khas yang mempunyai ciri-ciri keselamatan yang tinggi termasuk sistem pencegah kebakaran; ii. akses adalah terhad kepada pegawai yang telah diberi kuasa sahaja dan dipantau pada setiap masa; 	<p>Pentadbir Sistem ICT, Pihak Luaran dan Pengguna</p>
---	--


	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

<ul style="list-style-type: none"> iii. pemantauan dibuat menggunakan kamera CCTV atau lain-lain kaedah yang sesuai; iv. peralatan keselamatan (CCTV, log akses) perlu diperiksa secara berjadual; v. butiran pelawat yang keluar masuk ke kawasan larangan perlu direkodkan; vi. pelawat yang dibawa masuk mesti diiringi oleh pegawai yang bertanggungjawab sepanjang tempoh di lokasi berkaitan; dan vii. pihak luaran adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal dan hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai. 	
---	--


0502 Keselamatan Peralatan

Objektif:


Melindungi peralatan ICT jabatan daripada kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


050201 Peralatan ICT	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ul style="list-style-type: none"> i. pengguna hendaklah menyemak dan memastikan semua perkakasan ICT di bawah kawalannya berfungsi dengan sempurna; ii. pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; iii. pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan; iv. pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT; v. pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; vi. pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (<i>activated</i>) dan dikemaskini di samping melakukan imbasan ke atas media storan yang digunakan; 	Semua

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


<p>vii. penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;</p> <p>viii. semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran;</p> <p>ix. perkakasan ICT yang kritikal perlu disokong oleh <i>Uninterruptable Power Supply</i> (UPS) dan perlu diletakkan di bilik yang berasingan bersuhu rendah yang dilengkapi dengan pengudaraan yang sesuai;</p> <p>x. semua perkakasan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti <i>switches</i>, <i>hub</i>, <i>router</i> dan lain-lain perlu diletakkan di dalam rak khas dan berkunci;</p> <p>xi. semua peralatan yang digunakan secara berterusan hendaklah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (<i>air ventilation</i>) yang sesuai;</p> <p>xii. perkakasan ICT yang hendak dibawa keluar dari premis jabatan perlulah mendapat kelulusan Pentadbir Sistem ICT/Ketua Jabatan dan direkodkan bagi tujuan pemantauan;</p>	
---	--

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

<p>xiii. perkakasan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera;</p> <p>xiv. aset ICT yang hilang semasa di luar waktu pejabat hendaklah dikendalikan mengikut prosedur dan peraturan semasa yang sedang berkuatkuasa;</p> <p>xv. pengendalian perkakasan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;</p> <p>xvi. pengguna tidak dibenarkan mengubah perkakasan ICT dari tempat asal tanpa kebenaran Ketua Jabatan ICT/ Pentadbir Sistem ICT;</p> <p>xvii. sebarang kerosakan perkakasan ICT hendaklah dilaporkan kepada Pegawai Aset/Ketua Jabatan ICT untuk di baik pulih;</p> <p>xviii. sebarang pelekak selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin perkakasan tersebut sentiasa berkeadaan baik;</p> <p>xix. konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal;</p>	
--	--

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


<p>xx. pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (<i>administrator password</i>) yang telah ditetapkan oleh Pentadbir Sistem ICT;</p> <p>xxi. pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja;</p> <p>xxii. pengguna hendaklah memastikan semua perkakasan ICT dimatikan (<i>switch off</i>) apabila meninggalkan pejabat. Sebaiknya plag dicabut daripada suis utama (<i>main switch</i>) sebelum meninggalkan pejabat bagi mengelakkan kerosakan perkakasan ICT seperti komputer dan pencetak jika berlaku kejadian seperti petir, kilat dan sebagainya; dan</p> <p>xxiii. sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO.</p>	
050202 Media Storan	
<p>Media storan perlu berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p>	<p>Semua</p>

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


<ul style="list-style-type: none"> i. media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; ii. akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada pengguna yang dibenarkan sahaja; iii. semua media storan perlu dikawal bagi mencegah capaian yang tidak dibenarkan, kecurian dan kemusnahan; iv. semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan (<i>data safe</i>) yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet; v. akses dan pergerakan media storan hendaklah direkodkan; vi. perkakasan <i>backup</i> hendaklah diletakkan di tempat yang terkawal; vii. mengadakan salinan atau penduaan (<i>backup</i>) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data. Satu salinan pendua 	
---	--

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

<p>harus disimpan di bangunan berbeza dan di luar jabatan;</p> <p>viii. storan dan peralatan <i>backup</i> hendaklah disimpan di lokasi yang berasingan yang lebih privasi dan tidak terbuka kepada umum. Akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada pengguna yang dibenarkan sahaja;</p> <p>ix. semua media storan data yang hendak dilupuskan hendaklah dihapuskan dengan teratur dan selamat;</p> <p>x. penghapusan maklumat atau kandungan media hendaklah mendapat kelulusan pemilik maklumat terlebih dahulu; dan</p> <p>xi. pengguna hendaklah bertanggungjawab sepenuhnya dalam membuat salinan fail kerja harian ke dalam media storan peribadi.</p>	
050203 Media Tandatangan Digital	
<p>Perkara-perkara yang perlu dipatuhi adalah:</p> <p>i. pengguna hendaklah bertanggungjawab sepenuhnya ke atas media tandatangan digital bagi melindungi daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan;</p>	Semua

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


<ul style="list-style-type: none"> ii. media ini tidak boleh dipindah milik atau dipinjamkan; dan iii. sebarang insiden kehilangan yang berlaku hendaklah dilaporkan segera kepada ICTSO atau CERTNS untuk tindakan selanjutnya. 	
050204 Media Perisian dan Aplikasi (<i>Software</i>)	
<p>Perkara-perkara yang perlu dipatuhi adalah:</p> <ul style="list-style-type: none"> i. hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan di jabatan; ii. sistem aplikasi dalaman tidak dibenarkan di demonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran Pengurus ICT; iii. lesen perisian (<i>registration code, serials, CD-keys</i>) perlu disimpan berasingan daripada <i>CD-ROM, disk</i> atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; dan iv. <i>source code</i> sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan hendaklah mengikut prosedur yang ditetapkan. 	Semua

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

050205 Penyelenggaraan Perkakasan	
<p>Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Perkara-perkara yang perlu dipatuhi adalah:</p> <ul style="list-style-type: none"> i. semua perkakasan yang diselenggarakan hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar; ii. memastikan perkakasan hanya boleh diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja; iii. bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; iv. menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; v. memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; vi. semua penyelenggaraan hendaklah mendapat kebenaran daripada Pengurus ICT; dan vii. merekod kerja-kerja penyelenggaraan di dalam kad harta modal mengikut tatacara pengurusan aset. 	<p>Pengurus ICT dan Pegawai Aset</p>

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

050206 Peralatan di Luar Premis	
<p>Perkakasan yang dibawa keluar dari premis jabatan adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah:</p> <ul style="list-style-type: none"> i. perkakasan perlu dilindungi dan dikawal sepanjang masa; ii. penyimpanan atau penempatan perkakasan hendaklah mengambil kira ciri-ciri keselamatan yang bersesuaian; iii. setiap peralatan yang dibawa keluar premis wajib direkodkan; dan iv. sebarang kehilangan peralatan adalah di bawah tanggungjawab individu yang membawa keluar perkakasan tersebut. 	Pegawai Aset dan Pengguna
050207 Pelupusan Perkakasan	
<p>Pelupusan perkakasan ICT perlu dilakukan secara terkawal mengikut prosedur pelupusan di dalam Tatacara Pengurusan Aset Alih Kerajaan yang sedang berkuatkuasa. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p>	Pegawai Aset dan Pengguna

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

<ul style="list-style-type: none"> i. semua kandungan perkakasan khususnya maklumat rahsia rasmi hendaklah dihapuskan (sanitasi data/media) terlebih dahulu sebelum pelupusan dilaksanakan; ii. sekiranya maklumat perlu disimpan, maka pengguna boleh membuat penduaan (<i>backup</i>); iii. Pegawai Aset hendaklah mengenalpasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; iv. perkakasan yang hendak dilupus perlu disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan; v. data-data yang terkandung dalam storan perkakasan ICT yang akan dilupuskan sebelum dipindahmilik perlu dihapuskan dengan cara yang selamat; vi. Pegawai Aset bertanggungjawab merekodkan butir-butir pelupusan dan mengemaskini rekod pelupusan perkakasan ICT ke dalam kad harta modal mengikut tatacara pengurusan aset; vii. pelupusan perkakasan ICT hendaklah dilakukan secara berpusat dan mengikut prosedur pelupusan semasa yang berkuat kuasa; dan 	
--	--


	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

<p>viii. pengguna ICT adalah DILARANG SAMA SEKALI melakukan perkara-perkara berikut:</p> <ul style="list-style-type: none"> a. menyimpan mana-mana perkakasan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, <i>hardisk</i>, <i>motherboard</i> dan sebagainya; b. menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, <i>speaker</i> dan mana-mana peralatan yang berkaitan ke mana-mana jabatan/bahagian di premis jabatan; c. memindah keluar dari premis jabatan mana-mana perkakasan ICT yang hendak dilupuskan; d. melupuskan sendiri peralatan ICT; dan e. memastikan segala maklumat sulit dan rahsia di dalam peralatan disalin pada media storan kedua sebelum menghapuskan maklumat secara kekal. 	
---	--

0503 Keselamatan Persekitaran

Objektif:


Melindungi Aset ICT jabatan daripada sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaiian atau kemalangan.

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

050301 Kawalan Persekitaran	
<p>Bagi menghindarkan kerosakan dan gangguan terhadap premis dan Aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, mengubahsuai, membuat pembelian hendaklah dirujuk terlebih dahulu kepada ICTSO. Perkara-perkara berikut hendaklah dipatuhi:</p> <ul style="list-style-type: none"> i. merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti; ii. semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; iii. peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; iv. bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan Aset ICT; v. semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari Aset ICT; 	Pengguna

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


<p>vi. pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer;</p> <p>vii. semua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya dua (2) kali setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi rujukan dan tindakan sekiranya perlu; dan</p> <p>viii. akses kepada saluran <i>riser</i> hendaklah sentiasa dikunci.</p>	
050302 Bekalan Kuasa	
<p>Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <p>i. semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT;</p> <p>ii. peralatan sokongan seperti <i>Uninterruptable Power Supply</i> (UPS) dan penjana (<i>generator</i>) boleh digunakan bagi perkhidmatan kritikal seperti di pusat data/bilik <i>server</i> supaya mendapat bekalan kuasa berterusan; dan</p>	ICTSO dan PKJ

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

iii. semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual oleh pihak yang bertaualiah.	
050303 Kabel Komputer / Rangkaian	
<p>Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut:</p> <ul style="list-style-type: none"> i. menggunakan kabel komputer/rangkaian mengikut spesifikasi yang telah ditetapkan; ii. melindungi kabel komputer/rangkaian daripada kerosakan yang disengajakan atau tidak disengajakan; iii. melindungi laluan pemasangan kabel komputer/rangkaian sepenuhnya bagi mengelakkan ancaman kerosakan dan <i>wire tapping</i>; iv. kabel rangkaian perlu dilabelkan dengan jelas dan hendaklah melalui trunking bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat; dan v. penambahan/ perombakan/ <i>dismantle</i> kabel rangkaian perlu melalui Pentadbir Sistem ICT. 	ICTSO dan Pentadbir Sistem ICT

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


050304 Prosedur Kecemasan	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ul style="list-style-type: none"> i. setiap pegawai dan kakitangan hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Garis Panduan Keselamatan yang dikeluarkan oleh PKJ; dan ii. kecemasan persekitaran seperti kebakaran, banjir, keruntuhan bangunan dan sebagainya hendaklah dilaporkan kepada PKJ yang dilantik. 	PKJ
0504 Keselamatan Dokumen	
<p>Objektif:</p> <p>Melindungi maklumat jabatan daripada sebarang bentuk ancaman persekitaran disebabkan oleh bencana alam, kesilapan, kecuaiian dan kebocoran maklumat.</p>	
050401 Dokumen	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ul style="list-style-type: none"> i. setiap dokumen hendaklah difailkan dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar; 	Pegawai Pengelasan Dokumen dan Pegguna

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

<ul style="list-style-type: none"> ii. pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan; iii. kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan; iv. pelupusan dokumen hendaklah mengikut prosedur keselamatan yang sedang berkuatkuasa sepertimana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; v. semua dokumen terperingkat yang disediakan dan dihantar secara elektronik perlu menggunakan kaedah enkripsi (<i>encryption</i>); dan vi. memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan. 	
--	--

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

BIDANG 06 PENGURUSAN OPERASI DAN KOMUNIKASI	
0601 Pengurusan Prosedur Operasi	
Objektif: Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.	
060101 Pengendalian Prosedur	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: <ul style="list-style-type: none"> i. semua prosedur pengurusan operasi yang di diguna pakai hendaklah didokumen, disimpan dan dikawal; dan ii. setiap prosedur hendaklah mengandungi arahan-arahan yang jelas, teratur, lengkap dan hendaklah dikemas kini mengikut keperluan. 	Semua
060102 Kawalan Perubahan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: <ul style="list-style-type: none"> i. peningkatan atau pengubahsuaian yang melibatkan perkakasan, perisian, sistem rangkaian, sistem 	Pengurus ICT, Pentadbir Sistem ICT, Pegawai Aset dan

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

<p>aplikasi, dan prosedur hendaklah mendapat kebenaran daripada pegawai atasan;</p> <p>ii. aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemaskini mana-mana komponen Aset ICT hendaklah dikendalikan oleh pegawai atau pihak yang diberi kebenaran;</p> <p>iii. semua aktiviti pengubahsuaian Aset ICT hendaklah mematuhi spesifikasi yang telah ditetapkan;</p> <p>iv. semua aktiviti peningkatan dan pengubahsuaian hendaklah direkod untuk tujuan kawalan dan semakan semula; dan</p> <p>v. setiap perubahan yang dilakukan perlu mendapat kelulusan Pengurus ICT dan direkodkan.</p>	Pengguna
060103 Pengasingan Tugas dan Tanggungjawab	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <p>i. skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas Aset ICT;</p>	ICTSO, Pengurus ICT dan Pentadbir Sistem ICT

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

<p>ii. tugas mewujudkan, memadam, mengemaskini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi Aset ICT daripada kesilapan, kebocoran maklumat atau di manipulasi; dan</p> <p>iii. persekitaran perkakasan yang digunakan bagi tujuan pembangunan sistem aplikasi (<i>development/stagging</i>) dan penggunaan sebenar (<i>production</i>) hendaklah diasingkan.</p>	
---	--

0602 Pengurusan Penyampaian Perkhidmatan Pihak Luar

Objektif:


Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak luaran.

060201 Penyampaian Perkhidmatan


Perkara-perkara yang mesti dipatuhi adalah seperti berikut:

- memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang


Pengurus ICT,
Pentadbir
Sistem ICT
dan
Pihak Luar

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


<p>terkandung dalam perjanjian dilaksanakan dan diselenggarakan oleh pihak luaran;</p> <p>ii. perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak luaran perlu sentiasa dipantau, disemak semula dan diaudit oleh pegawai yang bertanggungjawab; dan</p> <p>iii. pengurusan kepada perubahan penyediaan perkhidmatan termasuk penyelenggaraan dan penambahan polisi keselamatan, prosedur dan kawalan maklumat sedia ada perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.</p>	
0603 Perancangan dan Penerimaan Sistem	
<p>Objektif:</p> <p>Meminimumkan risiko yang menyebabkan gangguan dan kegagalan sistem.</p>	
060301 Perancangan Kapasiti	
<p>Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang bertanggungjawab pada masa akan datang.</p>	<p>ICTSO, Pengurus ICT dan Pentadbir Sistem ICT</p>

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


Perancangan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko gangguan dan kegagalan perkhidmatan serta kerugian akibat pengubahsuaian yang tidak dirancang.	
060302 Penerimaan Sistem	
<ul style="list-style-type: none"> i. Semua sistem baharu dan diubah suai hendaklah memenuhi spesifikasi yang ditetapkan sebelum diterima pakai; ii. semua sistem baharu dan yang diubah suai hendaklah melalui peringkat pengujian <i>User Acceptance Test (UAT)</i>, <i>Provisional Acceptance Test (PAT)</i> & <i>Final Acceptance Test (FAT)</i> sebelum dilaksanakan; dan iii. dokumentasi sistem perlu disediakan, dikemaskini mengikut kawalan versi dan dibuat salinan serta disimpan di tempat yang selamat. 	Pentadbir Sistem ICT dan Pengguna
0604 Perisian Berbahaya	
<p>Objektif:</p> <p>Melindungi integriti perisian dan maklumat daripada pendedahan atau kerosakan disebabkan oleh perisian berbahaya seperti virus, <i>malware</i> dan sebagainya.</p>	

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


060401 Perlindungan Daripada Perisian Berbahaya	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> memasang sistem keselamatan seperti antivirus, <i>Intrusion Detection System (IDS)</i> dan <i>Intrusion Prevention System (IPS)</i> yang bersesuaian mengikut prosedur penggunaan yang betul dan selamat; memastikan paten antivirus pada perkakasan ICT dikemaskini dengan versi terkini; menggunakan perisian yang dilindungi di bawah undang-undang bertulis yang berkuat kuasa; mengimbas media storan dengan antivirus terkini sebelum menggunakannya; mengemaskini <i>patches</i> sistem operasi mengikut keperluan; menyemak fail sistem dan pangkalan data; memasukkan klausa tuntutan baik pulih dalam dokumen kontrak perjanjian; mengadakan program atau prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan 	<p>Pengurus ICT, Pentadbir Sistem ICT dan Pengguna</p>

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

ix. memaklumkan pengguna mengenai ancaman keselamatan ICT seperti serangan virus.	
060402 Perlindungan Daripada <i>Mobile Code</i>	
Penggunaan <i>mobile code</i> yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	Pengurus ICT dan Semua
0605 Housekeeping	
<p>Objektif:</p> <p>Meningkatkan prestasi capaian dan pemprosesan maklumat bagi memastikan kebolehsediaan data/maklumat dan melindungi integriti maklumat serta boleh diakses pada bila-bila masa.</p>	
060501 <i>Backup</i>	
<p>Proses salinan sistem aplikasi, data dan fail konfigurasi bagi memastikan sistem dapat beroperasi semula sekiranya diperlukan.</p> <p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <p>i. melaksanakan <i>backup</i> ke atas semua sistem aplikasi dan fail konfigurasi;</p>	Pentadbir Sistem ICT

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

<ul style="list-style-type: none"> ii. melaksanakan <i>backup</i> ke atas semua data secara berkala/berjadual; iii. menguji fail <i>backup</i> melalui prosedur <i>restore</i> bagi memastikan ianya berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; dan iv. merekod dan menyimpan salinan <i>backup</i> di lokasi yang berlainan dan selamat. 	
0606 Pengurusan Rangkaian	
<p>Objektif: Melindungi infrastruktur rangkaian dan maklumat.</p>	
060601 Kawalan Infrastruktur Rangkaian	
<p>Infrastruktur rangkaian hendaklah dikawal dan diuruskan bagi memastikan matlamat kerahsiaan, integriti dan ketersediaan tercapai. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ul style="list-style-type: none"> i. peralatan rangkaian hendaklah diletakkan di lokasi yang selamat; 	<p>Pengurus ICT dan Pentadbir Sistem ICT</p>

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


<ul style="list-style-type: none"> ii. perkakasan atau perisian keselamatan rangkaian hendaklah dipasang, dikonfigurasi dan diselaja; iii. konfigurasi peralatan keselamatan rangkaian hendaklah dirancang, diluluskan dan direkodkan; iv. semua trafik keluar dan masuk hendaklah melalui <i>firewall</i> di bawah kawalan jabatan; v. semua perisian penganalisa paket seperti <i>sniffer</i> atau <i>network analyser</i> adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO; vi. sebarang penyambungan rangkaian yang bukan di bawah kawalan jabatan adalah tidak dibenarkan; vii. penggunaan <i>modem</i>, <i>access point</i> dan <i>wireless broadband</i> persendirian hendaklah mendapat kebenaran ICTSO dan memaklumkan kepada pentadbir rangkaian. 	
0607 Pengurusan Media	
<p>Objektif: Melindungi Aset ICT daripada ancaman yang boleh menyebabkan gangguan terhadap perkhidmatan.</p>	

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

060701 Pengendalian Media	
<ul style="list-style-type: none"> i. Melabelkan semua media mengikut tahap keselamatan sesuatu maklumat; ii. penghantaran atau pemindahan media ke lokasi lain di luar pejabat hendaklah direkodkan dan mengikut jadual yang telah ditetapkan; iii. mengawal dan merekodkan aktiviti pengendalian media bagi mengelak daripada sebarang kerosakan dan pendedahan yang tidak dibenarkan; iv. menyimpan semua media di tempat yang selamat; dan v. pelupusan media hendaklah dikendalikan mengikut klasifikasi keselamatan media. 	Pegawai Aset dan Pengguna
0608 Pengurusan Pertukaran Maklumat	
<p>Objektif:</p> <p>Memastikan pertukaran maklumat di antara jabatan dan agensi luar adalah selamat dan terjamin.</p>	

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

060801 Pertukaran Maklumat	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ul style="list-style-type: none"> i. dasar dan prosedur kawalan pertukaran maklumat perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; dan ii. media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari premis jabatan; 	<p>Pengurus ICT dan Pentadbir Sistem ICT</p>
060802 Pengurusan Mel Elektronik (E-mel)	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ul style="list-style-type: none"> i. pengguna e-mel di jabatan hendaklah mematuhi etika penggunaan E-mel dan Internet yang terkandung dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “<i>Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan</i>”; ii. hanya e-mel rasmi jabatan sahaja dibenarkan dalam setiap urusan rasmi; 	<p>Pentadbir Sistem ICT dan Pengguna</p>

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

<p>iii. sebarang pemindahan dokumen terperingkat melalui e-mel hendaklah merujuk kepada bidang 0802 - Kawalan Kriptografi; dan</p> <p>iv. Jabatan perlu menyediakan polisi, prosedur atau arahan-arahan bertulis yang bersesuaian mengenai penggunaan e-mel.</p>	
--	--

0609 Perkhidmatan Pembayaran Dalam Talian

Objektif:

Mengawal sensitiviti aplikasi dan maklumat agar sebarang kemungkinan risiko dapat dielakkan.

060901 Pembayaran Atas Talian

Pembayaran atas talian ialah kemudahan transaksi pembayaran secara elektronik yang disediakan untuk mendapatkan perkhidmatan kerajaan.


Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- i. memastikan transaksi mempunyai ciri-ciri keselamatan yang bersesuaian, berintegriti, diuji secara komprehensif, mematuhi akta (PDPA) dan tatacara kewangan yang berkuatkuasa;

Pengurus ICT
dan
Pengguna

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


<p>ii. maklumat yang terlibat dalam transaksi perlu dilindungi daripada aktiviti penipuan dan pendedahan serta pengubahsuaian yang tidak dibenarkan; dan</p> <p>iii. maklumat yang terlibat perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan.</p>	
0610 Pemantauan	
<p>Objektif: Memastikan Aset ICT bebas daripada ancaman.</p>	
061001 Pengauditan dan Forensik ICT	
<p>Pegawai yang bertanggungjawab hendaklah merekod dan menganalisis/melaporkan perkara-perkara berikut:</p> <p>i. sebarang cubaan atau pencerobohan kepada Aset ICT jabatan;</p> <p>ii. serangan kod perosak (<i>malicious code</i>), halangan pemberian perkhidmatan (<i>denial of service</i>), <i>spam</i>, pemalsuan (<i>forgery</i>), pencerobohan (<i>intrusion</i>)</p>	<p>ICTSO, Pengurus ICT dan Pentadbir Sistem ICT</p>

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


<p>ancaman (<i>threats</i>) dan kehilangan fizikal (<i>physical loss</i>);</p> <p>iii. pengubahsuaian sesebuah Aset ICT tanpa pengetahuan, arahan atau persetujuan mana-mana pihak;</p> <p>iv. sebarang Insiden berkaitan keselamatan maklumat atau aset ICT jabatan seperti di bidang 0902 - Pengurusan Maklumat Insiden Keselamatan ICT;</p> <p>v. aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan;</p> <p>vi. aktiviti instalasi dan penggunaan perisian yang membebaskan jalur lebar (<i>bandwidth</i>);</p> <p>vii. aktiviti penyalahgunaan akaun e-mel;</p> <p>viii. aktiviti penukaran alamat IP (<i>IP address</i>) selain yang telah diperuntukkan tanpa kebenaran; dan</p> <p>ix. larangan memuat turun dan instalasi permainan komputer (<i>games</i>), <i>hacking tools</i>, video conference atau video <i>streaming</i> dan perisian yang tidak dibenarkan.</p>	
--	--

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


061002 Jejak Audit	
<p>Setiap sistem ICT hendaklah mempunyai jejak audit (<i>audit trail</i>) yang mengandungi maklumat-maklumat berikut:</p> <ol style="list-style-type: none"> rekod bagi setiap transaksi seperti identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan; maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan; jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat dan Akta Arkib Negara; jejak audit perlu dilindungi daripada kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan; dan Jabatan perlu menyediakan polisi, prosedur atau arahan-arahan bertulis sekiranya perlu. 	<p>Pentadbir Sistem ICT</p>

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

061003 Sistem Log	
<p>Pegawai yang bertanggungjawab hendaklah melaksanakan perkara-perkara berikut:</p> <ul style="list-style-type: none"> i. mewujudkan fail log bagi merekodkan aktiviti pengguna; ii. memantau, menyemak dan melaksanakan <i>housekeeping</i> sistem log secara berkala bagi mengesan ancaman yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan iii. pegawai yang bertanggung jawab hendaklah melaporkan kepada ICTSO sebarang insiden keselamatan. 	<p>Pentadbir Sistem ICT</p>
061004 Pemantauan Log	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ul style="list-style-type: none"> i. log audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; 	<p>Pengurus ICT dan Pentadbir Sistem ICT</p>

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

<ul style="list-style-type: none"> ii. maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan; iii. kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan, dianalisis dan diambil tindakan sewajarnya; dan iv. penentuan masa bagi sistem aplikasi perlu diselaraskan dengan satu sumber waktu yang dipersetujui. 	
--	--

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

BIDANG 07 KAWALAN CAPAIAN	
0701 Dasar Kawalan Capaian	
<p>Objektif: Mengawal capaian ke atas Aset ICT.</p>	
070101 Keperluan Kawalan Capaian	
<p>Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza.</p> <p>Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ul style="list-style-type: none"> i. kawalan capaian ke atas Aset ICT mengikut keperluan keselamatan dan peranan pengguna; ii. kawalan capaian ke atas perkhidmatan semua jenis rangkaian (tanpa wayar dan berwayar) dalaman dan luaran; iii. kawalan capaian maklumat menggunakan 	<p>Pengurus ICT dan Pentadbir Sistem ICT</p>

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

<p>kemudahan atau peralatan mudah alih; dan</p> <p>iv. kawalan ke atas kemudahan pemprosesan maklumat seperti <i>server</i>, komputer peribadi dan komputer riba.</p>	
---	--

0702 Pengurusan Capaian Pengguna

Objektif:


Mengawal capaian pengguna ke atas Aset ICT.

070201 Akaun Pengguna


Setiap pengguna adalah bertanggungjawab ke atas Aset ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, perkara berikut hendaklah dipatuhi:

- akaun yang diberikan oleh Pentadbir Sistem ICT sahaja boleh digunakan;
- akaun pengguna yang diwujudkan hendaklah unik dan mendapat kelulusan daripada Pentadbir Sistem ICT;
- pemilikan akaun pengguna bukanlah hak milik mutlak;
- penggunaan akaun milik orang lain atau akaun yang


Pentadbir
Sistem ICT
dan
Pengguna

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


<p>dikongsi bersama adalah dilarang; dan</p> <p>v. akaun pengguna boleh dibeku atau ditamatkan atas sebab berikut:</p> <ul style="list-style-type: none"> a. pengguna yang tidak aktif melebihi enam (6) bulan; b. bertukar bidang tugas kerja; c. bertukar ke jabatan lain; d. bersara; e. ditamatkan perkhidmatan; f. permohonan daripada pihak jabatan; atau g. disyaki berlaku salah guna. 	
070202 Hak Capaian	
<p>Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan berdasarkan keperluan skop tugas.</p>	<p>Pentadbir Sistem ICT</p>

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


070203 Pengurusan Kata Laluan	
<p>Pengurusan kata laluan hendaklah mematuhi prosedur yang ditetapkan seperti berikut:</p> <ol style="list-style-type: none"> kata laluan hendaklah dilindungi dan tidak boleh dikongsi; pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran; panjang kata laluan hendaklah sekurang-kurangnya dua belas (12) aksara dengan gabungan huruf, angka dan aksara khusus; kata laluan hendaklah diingat dan tidak boleh dicatat, disimpan atau didedahkan; kata laluan log masuk komputer dan <i>screen saver</i> hendaklah diaktifkan; kata laluan hendaklah tidak dipaparkan semasa input; kuatkuasakan pertukaran kata laluan semasa login kali pertama atau selepas kata laluan diset semula; kata laluan hendaklah berlainan daripada pengenalan 	<p>Pentadbir Sistem ICT dan Pengguna</p>

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


<p>identiti pengguna;</p> <p>ix. kata laluan hendaklah ditukar sekurang-kurangnya sekali dalam tempoh enam (6) bulan;</p> <p>x. mengelakkan penggunaan semula kata laluan yang terdahulu; dan</p> <p>xi. kata laluan pengguna hendaklah melalui proses enkripsi apabila disimpan di dalam pangkalan data.</p>	
070204 <i>Clear Desk dan Clear Screen</i>	
<p><i>Clear Desk dan Clear Screen</i> bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja atau di paparan skrin apabila pengguna tidak berada di tempatnya.</p> <p>Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <p>i. menggunakan kemudahan <i>password screen saver</i>, <i>logout</i> apabila meninggalkan komputer atau perisian yang bersesuaian;</p> <p>ii. menyimpan bahan-bahan sensitif di dalam laci atau</p>	<p>Pentadbir Sistem ICT dan Pengguna</p>

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


<p>kabinet fail yang berkunci;</p> <p>iii. memastikan semua dokumen diambil segera daripada pencetak, pengimbas, mesin faksimili dan mesin fotostat; dan</p> <p>iv. memastikan media storan mudah alih tidak ditinggalkan di komputer atau di ruang kerja.</p>	
0703 Kawalan Capaian Rangkaian	
<p>Objektif: Menghalang capaian tidak sah ke atas perkhidmatan rangkaian.</p>	
070301 Capaian Rangkaian	
<p>Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan:</p> <p>i. memasang peralatan yang bersesuaian antara rangkaian Pentadbiran Kerajaan Negeri Sembilan, rangkaian jabatan lain dan rangkaian awam;</p> <p>ii. mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya;</p>	<p>Pengurus ICT dan Pentadbir Sistem ICT</p>

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


<ul style="list-style-type: none"> iii. memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT; dan iv. mewujudkan segmentasi rangkaian untuk meningkatkan keselamatan dan mengawal permasalahan rangkaian. 	
070302 Capaian Internet	
<p>Capaian Internet hendaklah memenuhi keperluan etika penggunaan Internet yang terkandung dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan” dan undang-undang bertulis yang berkuat kuasa.</p> <p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ul style="list-style-type: none"> i. penggunaan Internet hendaklah dikawal secara berterusan oleh Pentadbir Sistem ICT bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja; ii. pemasangan peralatan mengikut keperluan dan bersesuaian untuk mengawal akses internet dan mengoptimumkan prestasi rangkaian; iii. penggunaan Internet hanya untuk kegunaan rasmi 	<p>ICTSO, Pengurus ICT, Pentadbir Sistem ICT dan Pengguna</p>

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


<p>sahaja;</p> <p>iv. bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Ketua Jabatan sebelum dimuat naik ke Internet; dan</p> <p>v. sebarang bahan yang dimuat turun daripada Internet hendaklah digunakan untuk tujuan yang dibenarkan.</p>	
0704 Kawalan Capaian Sistem Pengoperasian	
<p>Objektif: Menghalang capaian tidak sah ke atas sistem pengoperasian.</p>	
070401 Capaian Sistem Pengoperasian	
<p>Kemudahan keselamatan dalam sistem pengoperasian perlu digunakan untuk menghalang capaian ke sistem komputer iaitu:</p> <p>i. mengenal pasti identiti, setiap pengguna yang dibenarkan; dan</p> <p>ii. merekodkan capaian yang berjaya dan gagal.</p>	<p>ICTSO, Pengurus ICT dan Pentadbir Sistem ICT</p>

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

<p>Kaedah yang digunakan hendaklah mampu menyokong perkara berikut:</p> <ul style="list-style-type: none"> i. mengesahkan pengguna yang dibenarkan; ii. melaksana audit log ke atas semua capaian sistem pengoperasian; dan iii. menamatkan capaian sekiranya dibiarkan dalam keadaan <i>idle</i> dalam tempoh yang ditetapkan. 	
070402 Capaian Pihak Luaran	
<p>Sebarang capaian pihak luaran hendaklah:</p> <ul style="list-style-type: none"> i. mendapatkan kebenaran pegawai bertanggungjawab; ii. pegawai bertanggungjawab perlu memantau sepanjang aktiviti dilaksanakan; iii. pihak luaran hendaklah bertanggungjawab sepenuhnya terhadap sebarang insiden yang disebabkan oleh aktiviti yang dilakukan; dan iv. mematuhi semua peraturan dan undang-undang yang berkuatkuasa. 	<p>Pengurus ICT, Pentadbir Sistem ICT dan Pihak Luaran</p>

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

0705 Kawalan Capaian Data, Maklumat dan Sistem Aplikasi	
<p>Objektif:</p> <p>Menghalang capaian tidak sah ke atas data, maklumat dan sistem aplikasi.</p>	
070501 Capaian Data, Maklumat dan Sistem Aplikasi	
<p>Perkara-perkara berikut hendaklah dipatuhi:</p> <ul style="list-style-type: none"> i. pengguna hanya boleh menggunakan sistem aplikasi yang dibenarkan mengikut tahap capaian yang telah ditentukan; ii. setiap aktiviti capaian sistem aplikasi hendaklah direkodkan seperti di sub bidang 061002 – Jejak Audit; iii. menghadkan capaian sistem aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun pengguna akan disekat; dan iv. melaksanakan tambahan ciri-ciri keselamatan pada sistem aplikasi seperti penggunaan tandatangan digital, SSL dan CAPTCHA mengikut kesesuaian. 	<p>Pengurus ICT, Pentadbir Sistem ICT dan Pengguna</p>

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

0706 Peralatan Mudah Alih dan Kerja Jarak Jauh	
<p>Objektif:</p> <p>Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh.</p>	
070601 Peralatan Mudah Alih dan Kerja Jarak Jauh	
<p>Perkara yang perlu dipatuhi adalah seperti berikut:</p> <ul style="list-style-type: none"> i. peralatan mudah alih hendaklah disimpan di tempat yang selamat; ii. pergerakan peralatan mudah alih keluar daripada pejabat hendaklah mematuhi Tatacara Pengurusan Aset Alih Kerajaan; iii. tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan; dan iv. kawalan capaian dari luar terhadap sistem aplikasi dalaman hendaklah diberikan kepada pengguna yang dibenarkan sahaja. 	<p>Pengurus ICT, Pegawai Aset dan Pengguna</p>

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

**BIDANG 08 PEROLEHAN, PEMBANGUNAN DAN
PENYELENGGARAAN SISTEM APLIKASI**

0801 Keselamatan Dalam Membangunkan Sistem Aplikasi

Objektif:


Memastikan sistem aplikasi yang dibangunkan mempunyai ciri-ciri keselamatan ICT yang bersesuaian.

080101 Keperluan Keselamatan Sistem Aplikasi

Perkara yang perlu dipatuhi adalah seperti berikut:

- i. perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem aplikasi hendaklah mengambilkira kawalan keselamatan bagi memastikan tiada masalah atau ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat;
- ii. ujian keselamatan hendaklah dijalankan ke atas input data sistem aplikasi untuk menyemak pengesahan dan integriti data yang dimasukkan. Pengujian ke atas sistem pemprosesan untuk menentukan sama ada program berjalan mengikut proses kerja yang betul serta sistem output untuk memastikan data yang dihasilkan adalah tepat;

ICTSO,
Pentadbir
Sistem
Aplikasi,
dan
Pemilik
Sistem

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

<p>iii. sistem aplikasi perlu mengandungi semakan pengesahan (<i>validation</i>) untuk memastikan data yang dimasukkan mengikut format yang betul, sah dan berintegriti; dan</p> <p>iv. semua sistem aplikasi yang dibangunkan sama ada secara dalaman atau luaran hendaklah diuji secara keseluruhan bagi memastikan sistem berkenaan mematuhi aspek keselamatan yang telah ditetapkan.</p>	
080102 Pengesahan Data <i>Input</i> dan <i>Output</i>	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <p>i. data <i>input</i> sistem aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul;</p> <p>ii. data <i>output</i> daripada sistem aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat; dan</p> <p>iii. verifikasi data hendaklah dibuat apabila berlaku proses migrasi dan pindahan data sistem aplikasi.</p>	<p>Pentadbir Sistem Aplikasi dan Pengguna Sistem</p>

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

0802 Kawalan Kriptografi

Objektif:

Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.

080201 Enkripsi

Sistem Aplikasi yang melibatkan maklumat terperingkat hendaklah dibuat enkripsi (*encryption*).

Pentadbir
Sistem
Aplikasi
dan
Pengguna

080202 Tandatangan Digital


Maklumat terperingkat yang perlu diproses dan dihantar secara elektronik hendaklah menggunakan tandatangan digital mengikut keperluan pelaksanaan.

Pentadbir
Sistem ICT
dan
Pengguna

080203 Pengurusan Infrastruktur Kunci Awam (PKI)

Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan

Pentadbir
Sistem ICT

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

daripada diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	dan Pengguna
0803 Keselamatan Fail Sistem Aplikasi	
<p>Objektif:</p> <p>Memastikan supaya fail sistem aplikasi dikawal dan dikendalikan dengan baik dan selamat.</p>	
080301 Kawalan Fail Sistem Aplikasi	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ul style="list-style-type: none"> i. mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian fail sistem aplikasi; dan ii. sistem aplikasi hendaklah mempunyai fungsi jejak audit merujuk kepada sub bidang 061002 – Jejak Audit. 	Pengurus ICT dan Pentadbir Sistem ICT

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

0804 Keselamatan Proses Pembangunan dan Penyelenggaraan

Objektif:

Menjaga dan menjamin keselamatan sistem aplikasi.

080401 Prosedur Kawalan Perubahan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- i. penambahbaikan atau pengubahsuaian ke atas fungsi atau modul sistem aplikasi hendaklah diuji, direkod dan disahkan sebelum digunakan;
- ii. melaksanakan pengemaskinian ke atas perisian yang digunakan mengikut keperluan; dan
- iii. mengawal kawalan versi sistem mengikut keperluan Jabatan/Agensi.


Pengurus ICT
dan
Pentadbir
Sistem ICT

080402 Pembangunan Sistem Aplikasi Secara *Outsource*

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- i. pembangunan sistem aplikasi secara *outsource* perlu diselia oleh pentadbir dan pemilik sistem;

Pengurus ICT
dan
Pentadbir
Sistem ICT

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

<ul style="list-style-type: none"> ii. kod sumber bagi sistem aplikasi merupakan hak milik jabatan dan boleh diakses serta boleh dibuat perubahan oleh jabatan; iii. semua capaian yang dibenarkan kepada pihak luaran hendaklah mengikut keperluan jabatan; dan iv. pihak luaran hendaklah menyediakan dokumentasi lengkap sistem aplikasi mengikut keperluan dan tempoh yang telah ditetapkan oleh jabatan. 	
--	--

0805 Kawalan *Vulnerability* Teknikal

Objektif:

Memastikan kawalan *vulnerability* teknikal adalah sistematik dan berkesan.

080501 Kawalan Ancaman Teknikal

<p>Kawalan ancaman teknikal perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi dengan mematuhi perkara berikut:</p> <ul style="list-style-type: none"> i. memperoleh maklumat <i>vulnerability</i> teknikal yang tepat ke atas sistem aplikasi; ii. menilai <i>vulnerability</i> bagi mengenal pasti tahap risiko; dan iii. mengambil langkah kawalan untuk mengatasi risiko. 	<p>Pengurus ICT dan Pentadbir Sistem ICT</p>
---	--

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

BIDANG 09 PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

0901 Mekanisme Pelaporan Insiden Keselamatan ICT

Objektif:

Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden.


090101 Mekanisme Pelaporan

Insiden keselamatan ICT bermaksud musibah (*adverse event*) atau ancaman kemungkinan berlaku ke atas Aset ICT secara sengaja atau tidak.

Insiden keselamatan ICT hendaklah dilaporkan kepada ICTSO atau CERTNS dengan kadar segera apabila berlakunya perkara seperti berikut:

- i. maklumat didapati hilang atau disyaki hilang kepada pihak yang tidak bertanggungjawab;
- ii. maklumat didapati didedahkan atau disyaki didedahkan kepada pihak-pihak yang tidak diberi kuasa capaian;
- iii. sistem aplikasi digunakan tanpa kebenaran atau

ICTSO,
CERTNS
dan
Pengguna

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

<p>disyaki sedemikian;</p> <ul style="list-style-type: none"> iv. kawalan akses hilang, dicuri, diseleweng, didedahkan atau disyaki sedemikian; dan v. berlaku insiden pada sistem aplikasi atau sistem rangkaian yang luar daripada kebiasaan. <p>Ringkasan bagi semua proses kerja yang terlibat dalam pelaporan insiden seperti di Lampiran 4. Prosedur pelaporan insiden keselamatan ICT berdasarkan:</p> <ul style="list-style-type: none"> i. Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; ii. Surat Pekeliling Am Bilangan 4 Tahun 2006 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam; dan iii. Pemakluman Pelaksanaan Fungsi Pengurusan Pengendalian <i>Government Computer Emergency Response Team</i> (GCERT) Oleh Agensi Keselamatan Siber Negara (NACSA). 	
---	--

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

0902 Pengurusan Maklumat Insiden Keselamatan ICT

Objektif:


Memastikan insiden keselamatan ICT diuruskan dengan sistematik dan berkesan.

090201 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT

Maklumat mengenai insiden keselamatan ICT perlu dikendalikan, direkod, disimpan dan dianalisis bagi tujuan perancangan, tindakan pembetulan dan pengukuhan. Kawalan pengurusan pengendalian insiden seperti berikut:

- setiap insiden hendaklah dilaporkan dengan mengisi Borang Pelaporan Insiden dan diserahkan kepada pasukan CERTNS untuk tindakan susulan;
- menyimpan jejak audit, fail *backup* secara berkala dan melindungi integriti semua bahan bukti di tempat yang selamat;
- menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan;
- menyediakan pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan;

ICTSO,
CERTNS,
Pengurus ICT
dan
Pentadbir
Sistem ICT

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

<p>v. menyediakan tindakan pemulihan segera; dan</p> <p>vi. memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.</p>	
--	--

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

BIDANG 10 PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

1001 Dasar Kesinambungan Perkhidmatan

Objektif:

Memastikan penyampaian perkhidmatan yang berterusan kepada pelanggan.

100101 Pelan Kesinambungan Perkhidmatan (PKP)


PKP hendaklah dibangunkan untuk memastikan pendekatan menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. PKP dilaksanakan bagi memulihkan perkhidmatan secara formal supaya Jabatan/Agensi dapat meneruskan operasi sekiranya berlaku gangguan ICT yang berpanjangan.

Langkah berikut perlu dilakukan sebelum membangunkan PKP:


1. Penilaian Risiko Jabatan

Penilaian risiko perlu dilakukan bagi mengenalpasti perkhidmatan utama (*core business*), proses kritikal dan tahap risiko jabatan. Ancaman dan risiko ini boleh mengakibatkan gangguan terhadap perkhidmatan serta memberi impak terhadap fungsi kritikal jabatan. Hasil penemuan perlu didokumenkan dalam Laporan Penilaian Risiko.

Penyelaras
PKP

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


<p>2. Analisis Impak Perkhidmatan Jabatan</p> <p>Analisis Impak Perkhidmatan perlu dijalankan bagi mengenal pasti fungsi-fungsi kritikal perkhidmatan, tempoh pemulihan dan sumber operasi serta kewangan yang diperlukan. Ini bagi menentukan tahap toleransi jabatan sekiranya terdapat gangguan kepada fungsi berkenaan.</p> <p>Pelan PKP yang dibangunkan dan hendaklah mengandungi perkara-perkara berikut:</p> <ul style="list-style-type: none"> i. senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan; ii. senarai Pengurus ICT Pentadbiran Kerajaan Negeri Sembilan dan pihak luaran berserta nombor yang boleh dihubungi (faksimili, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan Pengurus ICT tidak dapat hadir untuk menangani insiden; iii. senarai lengkap maklumat yang memerlukan <i>backup</i> dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan; iv. alternatif sumber pemprosesan dan lokasi untuk 	
---	--

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


<p>menggantikan sumber yang telah lumpuh; dan</p> <p>v. perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan di mana boleh.</p> <p>Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini hendaklah diluluskan oleh Mesyuarat Pengurusan Jabatan. Perkara yang perlu dipatuhi adalah seperti berikut:</p> <p>i. mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan;</p> <p>ii. mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan ICT;</p> <p>iii. melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan;</p> <p>iv. mendokumentasikan proses dan prosedur yang telah dipersetujui;</p>	
--	--

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

<p>v. mengadakan program latihan kepada pengguna mengenai prosedur kecemasan;</p> <p>vi. salinan pelan PKP perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama dan sentiasa dikemas kini mengikut pelan utama;</p> <p>vii. menguji dan mengemas kini pelan apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan; dan</p> <p>viii. ujian PKP hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan.</p> <p>Pembangunan PKP hendaklah merujuk kepada dokumen Pengurusan Kesenambungan Perkhidmatan Agensi Sektor Awam yang dilampirkan bersama surat arahan Ketua Pengarah MAMPU (Rujukan MAMPU.BPICT.700-4/2/11 (3) bertarikh 22 Januari 2010.</p>	
100102 Pelan Pemulihan Bencana (<i>Disaster Recovery Plan</i>)	
<p>Pelan Pemulihan Bencana (<i>Disaster Recovery Plan</i> – DRP) direka bentuk untuk membantu jabatan mengembalikan semula</p>	<p>Penyelaras DRP</p>

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


<p>proses perkhidmatan dalam tempoh ditetapkan untuk pemulihan bencana.</p> <p>Ia merujuk kepada dokumen pelan yang menetapkan sumber, tindakan, tanggungjawab dan data yang diperlukan untuk mengurus proses pemulihan selepas berlaku gangguan dalam perkhidmatan agensi. Pelan ini mestilah diluluskan oleh pengurusan atasan Pentadbiran Kerajaan Negeri Sembilan dan perkara-perkara berikut perlu diberi perhatian:</p> <ul style="list-style-type: none"> i. mengenal pasti pejabat alternatif dan/atau pusat pemulihan bencana (<i>Disaster Recovery Centre – DRC</i>) yang berbeza dari lokasi asal bagi meneruskan perkhidmatan apabila lokasi asal menghadapi gangguan/bencana; ii. mengenalpasti peranan dan tanggungjawab Pasukan Pemulihan Bencana serta pihak luaran berkaitan; iii. mengenalpasti senarai sistem aplikasi kritikal yang memerlukan <i>backup</i> dan perlu diberi keutamaan serta mendokumentasi proses dan prosedur yang digunapakai untuk pemulihan maklumat sistem terlibat di dalam dokumen DRP; iv. menyediakan infrastruktur bagi memastikan pemulihan boleh dilaksanakan; 	
--	--

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

v. melaksanakan pengujian DRP dan latihan kepada kakitangan terlibat; dan	
vi. mengemaskini pelan sekiranya terdapat perubahan.	

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

BIDANG 11 PEMATUHAN	
1101 Pematuhan dan Keperluan Perundangan	
<p>Objektif:</p> <p>Meningkatkan tahap keselamatan ICT dan mengelakkan pelanggaran DKICT Pentadbiran Kerajaan Negeri Sembilan.</p>	
110101 Pematuhan Dasar	
<p>DKICT Pentadbiran Kerajaan Negeri Sembilan hendaklah dibaca, difahami dan dipatuhi.</p> <p>Ketua Jabatan berhak untuk memantau aktiviti pengguna terhadap aset ICT selain tujuan yang telah ditetapkan.</p> <p>Sebarang penggunaan Aset ICT selain maksud dan tujuan yang telah ditetapkan, merupakan satu kesalahan.</p>	Pengguna
110102 Pematuhan Dasar, Piawaian dan Prosedur	
Pegawai bertanggungjawab hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan prosedur.	CIO, ICTSO, Pengurus ICT dan Pentadbir Sistem ICT

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


110103 Pematuhan Keperluan Audit	
Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan.	Pengguna
110104 Dokumen Perundangan	
Dokumen perundangan yang perlu dipatuhi adalah seperti di Lampiran 5.	Pengguna
110105 Pelanggaran Dasar	
Pelanggaran DKICT Pentadbiran Kerajaan Negeri Sembilan serta semua perbuatan kecuai dan kelalaian yang membahayakan perkara-perkara terperingkat di bawah Akta Rahsia Rasmi 1972 dan akta lain yang berkaitan akan dikenakan tindakan undang-undang dan tatatertib.	Pengguna

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


GLOSARI	
<i>Antivirus</i>	Perisian yang mengimbas virus pada media storan seperti disket, cakera padat, pita magnetik, <i>optical disk</i> , <i>flash disk</i> , CDROM, <i>thumb drive</i> untuk sebarang kemungkinan adanya virus.
Aset Alih	Bermaksud aset yang boleh dipindahkan dari satu tempat ke satu tempat yang lain termasuk aset yang dibekalkan atau dipasang bersekali dengan bantuan.
Aset ICT	Terdiri daripada perkakasan, perisian, aplikasi sistem, perkhidmatan, data, maklumat, manusia, media storan, dokumentasi, premis komputer dan peralatan rangkaian.
<i>Backup</i>	Proses penduaan sesuatu dokumen atau maklumat.
<i>Bandwidth</i>	Jalur Lebar - Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
Biometrik	Kaedah yang digunakan untuk pengecaman identiti individu melalui pengesanan seperti cap jari, suara dan retina.
<i>CAPTCHA</i>	<i>Completely Automated Public Turing test to tell Computers and Humans Apart</i>

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


	Bertujuan untuk membezakan antara mesin (bot) dan manusia.
<i>CCTV</i>	<i>Closed-Circuit Television</i> – Sistem TV yang digunakan secara komersial di mana satu sistem TV kamera video dipasang di dalam premis pejabat bagi tujuan membantu pemantauan fizikal.
<i>Clear Desk dan Clear Screen</i>	Tidak meninggalkan dokumen data dan maklumat dalam keadaan terdedah di atas meja atau di paparan skrin komputer apabila pengguna tidak berada di tempatnya.
CERTNS	<i>Computer Emergency Response Team Negeri Sembilan</i> .Pasukan yang ditubuhkan untuk mengendalikan insiden keselamatan ICT di bawah Pentadbiran Kerajaan Negeri Sembilan.
CIO	<i>Chief Information Officer</i> - Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
<i>Denial of Service</i>	Halangan pemberian perkhidmatan.
<i>Downloading</i>	Aktiviti muat-turun sesuatu perisian.
<i>DRC</i>	<i>Disaster Recovery Centre</i> – Pusat Pemulihan Bencana
<i>DRP</i>	<i>Disaster Recovery Plan</i> – Pelan Pemulihan Bencana

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


<i>Encryption</i>	Enkripsi ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
<i>Final Acceptance Test (FAT)</i>	Ujian Penerimaan Akhir (FAT) adalah penilaian yang dilakukan semasa fasa pentauliahan oleh pihak ketiga yang melibatkan keseluruhan projek bagi menentukan prestasi dan keupayaan projek sebelum diguna pakai.
<i>Firewall</i>	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
<i>Forgery</i>	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel penyalahgunaan dan pencurian identiti, pencurian maklumat (<i>information theft/espionage</i>), penipuan (<i>hoaxes</i>).
GCERT	<i>Government Computer Emergency Response Team</i> atau Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan – Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya.
<i>Hacking Tool</i>	Program yang direka untuk membantu penggodaman, atau yang boleh digunakan untuk tujuan penggodaman.

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

<i>Hard Disk</i>	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.
<i>Hub</i>	Hab (<i>hub</i>) merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (<i>broadcast</i>) data yang diterima daripada sesuatu <i>port</i> kepada semua <i>port</i> yang lain.
ICT	<i>Information and Communication Technology</i> (Teknologi Maklumat dan Komunikasi).
ICTSO	<i>ICT Security Officer</i> - Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
<i>Idle</i>	Keadaan atau sesuatu yang tidak aktif.
Insiden Keselamatan	Musibah (<i>adverse event</i>) yang berlaku ke atas sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (<i>server</i>) atau komputer lain.
<i>Internet Gateway</i>	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan.

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


<i>Intrusion Detection System (IDS)</i>	Sistem Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat <i>host</i> atau rangkaian.
<i>Intrusion Prevention System (IPS)</i>	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/ atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau <i>malicious code</i> . Contohnya: <i>Network-based IPS</i> yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
Kriptografi	Kaedah untuk menukar data dan maklumat biasa (standard format) kepada format yang tidak boleh difahami bagi melindungi penghantaran data dan maklumat.
LAN	<i>Local Area Network</i> – Rangkaian Kawasan Setempat yang menghubungkan komputer.
<i>Logout</i>	<i>Log-out</i> komputer – Keluar daripada sesuatu sistem atau aplikasi komputer.
<i>Malicious Code</i>	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, <i>trojan horse</i> , <i>worm</i> , <i>spyware</i> dan sebagainya.

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


Media Tandatangan Digital	Satu mekanisma yang digunakan untuk menandatangani sesuatu dokumen rasmi secara elektronik.
<i>Mobile Code</i>	Merupakan suatu perisian yang boleh dipindahkan di antara sistem komputer dan rangkaian serta dilaksanakan tanpa perlu melalui sebarang proses pemasangan sebagai contoh Java Applet, ActiveX dan sebagainya pada pelayar internet.
MODEM	MODulator DEModulator - Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer.
NACSA	<i>National Cyber Security Agency</i> – Agensi Keselamatan Siber Negara
<i>Outsource</i>	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
Pegawai Aset	Pegawai yang dilantik untuk menjaga dan menguruskan aset.
Pegawai Keselamatan Jabatan	Pegawai yang bertanggungjawab mengenai pentadbiran Jabatan untuk melaksanakan arahan-arahan keselamatan Kerajaan dengan berhubung rapat dan mendapat nasihat dari Pegawai Keselamatan Kerajaan

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


Pengguna	Pegawai dan kakitangan yang bertanggungjawab menggunakan sistem
Pengurus ICT	Pegawai yang bertanggungjawab menguruskan keselamatan ICT di bawah kawalannya.
Pentadbiran Kerajaan Negeri Sembilan	Semua jabatan dan agensi termasuk Badan Berkanun Negeri dan Pihak Berkuasa Tempatan
Pentadbir Sistem ICT	Pegawai yang bertanggungjawab sebagai Pentadbir Rangkaian dan Keselamatan/ Pentadbir Sistem Aplikasi/ Pentadbir Laman Web (Webmaster)/ Pentadbir Pangkalan Data, Pentadbir Pusat Data dan Pentadbir E-mel.
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti <i>spreadsheet</i> dan <i>word processing</i> ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
Pihak Luaran	Terdiri daripada pembekal, pakar runding dan pihak-pihak lain yang terlibat dalam penggunaan atau capaian kepada aset dan perkhidmatan ICT Jabatan.
PKP	Pelan Kesyinambungan Perkhidmatan
<i>Provisional Acceptance Test (PAT)</i>	Fasa Ujian Penerimaan Sementara adalah penerimaan bersyarat yang bermaksud bahawa pengguna telah menerima projek tetapi prestasi perlu disahkan atau disahkan dalam tempoh yang telah dipersetujui.

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

<i>Public-Key Infrastructure (PKI)</i>	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
<i>Restoration</i>	Pemulihan ke atas data.
<i>Router</i>	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
<i>Screen Saver</i>	Imej yang akan diaktifkan pada komputer sekiranya tidak digunakan dalam jangka masa tertentu.
<i>SSL</i>	<i>Secure Socket Layer</i> merupakan protokol kriptografi yang digunakan dalam keselamatan komunikasi melalui internet.
<i>Server</i>	Pelayan komputer
<i>Switches</i>	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian <i>Carrier Sense Multiple Access/Collision Detection</i> (CSMA/CD) yang merupakan satu protokol penghantaran dengan mengurangkan perlanggaran yang berlaku.
<i>Uninterruptible Power Supply (UPS)</i>	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan daripada sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

<i>User Acceptance Test (UAT)</i>	Fasa pembangunan sistem aplikasi/perisian di mana sistem aplikasi/perisian tersebut diuji dalam "dunia nyata" oleh pengguna.
<i>Video Conference</i>	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.
<i>Video Streaming</i>	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
WAN	<i>Wide Area Network</i> – Rangkaian yang merangkumi kawasan yang luas.
<i>Wireless LAN</i>	Jaringan komputer yang terhubung tanpa melalui kabel.

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

LAMPIRAN 1



SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT (DKICT) PENTADBIRAN KERAJAAN NEGERI SEMBILAN VERSI 3.0

Nama (Huruf Besar) :

No. Kad Pengenalan :

Jawatan :

Jabatan/Agensi/Bahagian/Unit :

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:-

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam DKICT Pentadbiran Kerajaan Negeri Sembilan; dan
2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.


Tandatangan :

Tarikh :

Pengesahan

.....

Ketua Pegawai Maklumat (CIO)

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019


LAMPIRAN 2

NON-DISCLOSURE AGREEMENT

This agreement is entered into effective as of _____ between State Government of Negeri Sembilan and _____ Contractor is acting as an expert advising the State Government of Negeri Sembilan in connection with an _____

_____ and for that purpose the State Government of Negeri Sembilan may make certain Confidential Information (as define below) available to the Contractor (the “Purpose”). As a condition to, and in consideration of, the State Government of Negeri Sembilan furnishing of Confidential Information to the Contractor, the Contractor agrees to the restrictions and undertakings contained in this Agreement.


Contractor agrees that all information disclosed by the State Government of Negeri Sembilan to Contractor including any such information disclosed prior to the date of this Agreement, and including without limitation information acquired by Contractor in writing orally or by inspection of the State Government of Negeri Sembilan property, relating to (without limitation) the State Government of Negeri Sembilan samples, products, product plans, services, software invitation, process, discoveries, formulas, architectures, concepts, ideas, designs, drawings, personnel, customers, financial information, sales or programming matter, compositions, drawings, diagrams, computer programs, studies, work in process, confidential information disclosed to the Government of Negeri Sembilan by third parties and other data, whether oral, written, graphic or electronic form shall be considered “Confidential Information”.

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

Contractor agrees (i) to use Confidential Information solely for the Purpose, (ii) to use all possible means to maintain the Confidential Information in strict confidence, and at least those measures that it employs for the protection of its own confidential information, but in any event not less than a reasonable degree of care, (iii) to disclose information for the purpose and have previously signed an agreement in content similar to the provisions hereof; and (iv) to immediately notify in writing the State Government of Negeri Sembilan in the event of any unauthorized use or disclosure of the Confidential Information. Contractor shall not reverse engineer, disassemble, decompile or copy any software or other tangible objects, which embody the Confidential Information, nor export or re-export or otherwise transmit, directly or indirectly, any Confidential Information, or the direct product of Confidential Information.

All Confidential Information and all of the Contractor trademarks remain the property of the Contractor and no license or other rights in the Confidential Information or such trademarks are granted hereby, except as expressly provided above. This Agreement does not constitute a joint venture or other such business agreement. All information provided "as is" and without any warranty, express, implied or otherwise, regarding its accuracy or performance.

Contractor agrees to return to the State Government of Negeri Sembilan immediately upon the Contractor written request all documents and other tangible objects or representing the Confidential Information and all copies thereof which are in the possession of Contractor, including but not limited to all computer programs, documentation, notes, plans and drawing, and any reports, presentations, memorandums and other similar work made by Contractor in connection with or relating to the State Government of Negeri Sembilan or the Confidential Information. With respect to Confidential Information stored in


	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

electronic form in a writing signed by an authorized representative of Contractor that all Confidential Information has been deleted.

Contractor hereby acknowledges that unauthorized disclosure or use of Confidential Information could cause irreparable harm and significant injury, which may be difficult to ascertain. Accordingly, Contractor agrees that the State Government of Negeri Sembilan shall have the right to seek and obtain immediate injunctive relief from breaches of this Agreement, in addition to any other rights and remedies it may have.

Contractor obligations hereunder shall survive termination or expiration of this agreement until such time as all Confidential Information disclosed becomes publicly known and made generally available through no action or inaction of Contractor.

This Agreement shall bind and inure to the benefit of parties hereto and their successors and assigns, except that Confidential Information and the rights and obligations under this Agreement may not be assigned by Contractor without prior written consent of the Government of Negeri Sembilan. This document contains the entire agreement between the parties with respect to the subject matter hereof, and may not be amended, nor any obligation waived, except by a writing signed by both parties hereto. Any failure to enforce any provision of this Agreement shall not constitute a waiver thereof or any other provision. This Agreement shall be governed by and construed and enforced in accordance with the laws of the Government of Negeri Sembilan.

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

UNDERSTOOD AND AGREED:

For and on behalf of the)

GOVERNMENT OF NEGERI)

SEMBILAN DARUL KHUSUS)

.....

Designation)

I.C NO:)

For and on behalf of the)

)

.....

Name)

Designation:)

I.C NO)


In the presence of)

Name)

.....

Designation)

I.C NO)

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

LAMPIRAN 3

PERAKUAN UNTUK DITANDATANGANI OLEH SYARIKAT BERKENAAN DENGAN AKTA RAHSIA RASMI 1972

Adalah saya dengan ini mengaku bahawa perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 dan bahawa saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah, sesuatu benda rahsia, tidak menjaga dengan cara yang berpatutan sesuatu rahsia atau apa-apa tingkahlaku yang membahayakan keselamatan atau rahsia sesuatu benda rahsia adalah menjadi suatu kesalahan di bawah Akta tersebut, yang boleh dihukum maksimum penjara seumur hidup.

Saya faham bahawa segala maklumat rasmi yang saya perolehi dalam perkhidmatan Seri Paduka Baginda Yang di-Pertuan Agong atau perkhidmatan mana-mana Kerajaan dalam Malaysia, adalah milik Kerajaan dan tidak akan membocorkan, menyiarkan, atau menyampaikan, sama ada secara lisan atau dengan bertulis, kepada sesiapa jua dalam apa-apa bentuk, kecuali pada masa menjalankan kewajipan-kewajipan rasmi saya, sama ada dalam masa atau selepas perkhidmatan saya dengan Seri Paduka Baginda Yang di-Pertuan Agong atau dengan mana-mana Kerajaan dalam Malaysia dengan tidak terlebih dahulu mendapat kebenaran bertulis pihak berkuasa yang berkenaan. Saya berjanji dan mengaku akan menandatangani suatu akuan selanjutnya bagi maksud ini apabila meninggalkan Perkhidmatan Kerajaan.

Tandatangan:.....

Nama dengan huruf besar:.....

No. Kad Pengenalan:.....

Jawatan:.....

Syarikat:.....

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

Tarikh:.....

Disaksikan oleh:.....
(Tandatangan)

Nama dengan huruf besar:.....


No. Kad Pengenalan:.....

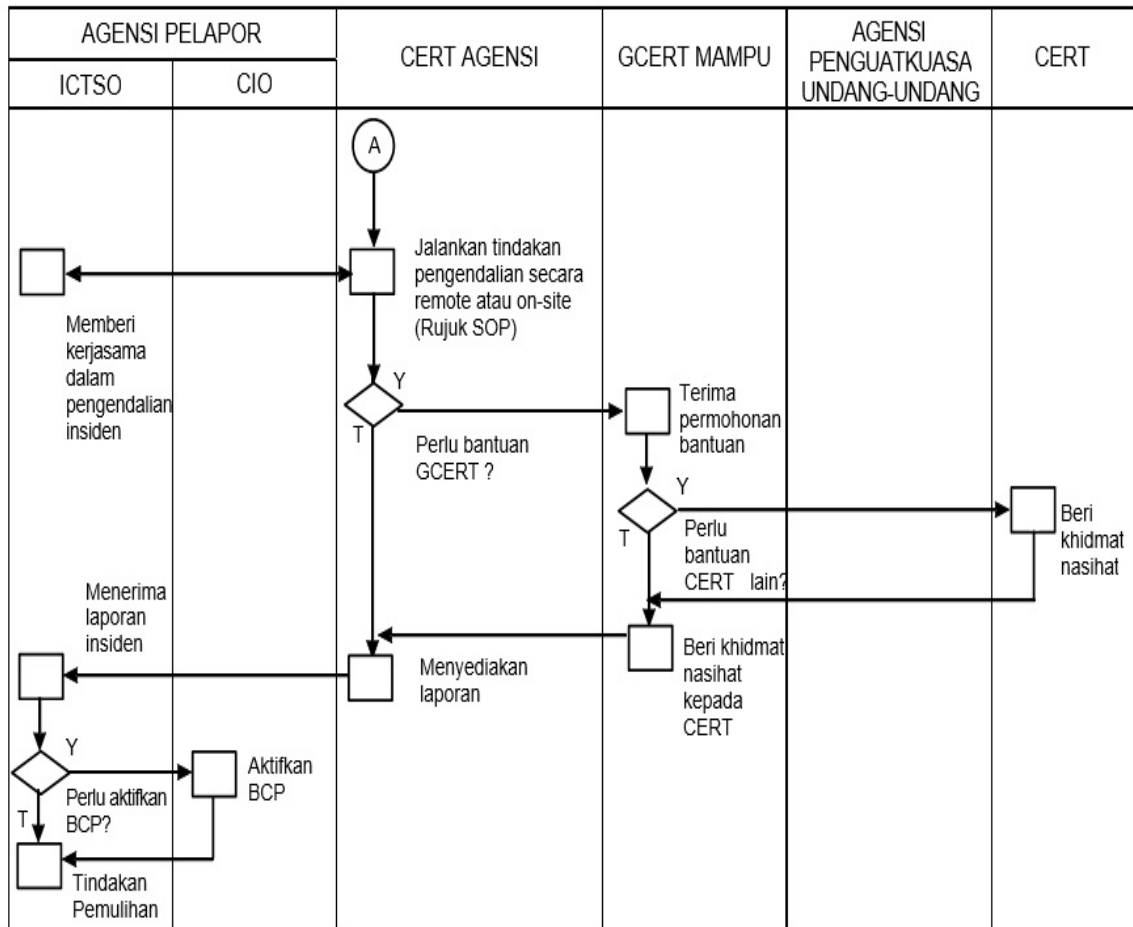
Jawatan:.....


Jabatan:.....

Tarikh:.....

Cop Jabatan:.....

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019



	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

Lampiran 5


DOKUMEN PERUNDANGAN	
1)	Arahan Keselamatan;
2)	Arahan Perbendaharaan;
3)	Arahan Teknologi Maklumat 2007;
4)	Perintah-Perintah Am;
5)	Surat Akujanji;
6)	Akta Rahsia Rasmi 1972;
7)	Akta Tandatangan Digital 1997;
8)	Akta Jenayah Komputer 1997;
9)	Akta Hak Cipta (Pindaan) Tahun 1997;
10)	Akta Komunikasi dan Multimedia 1998;
11)	Pelan Kesenimbangan Perkhidmatan;
12)	Pelan Pemulihan Bencana;
13)	Polisi Penggunaan E-mel Pentadbiran Kerajaan Negeri Sembilan;

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

14)	Dasar Keselamatan ICT Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU);
15)	Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;
16)	Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);
17)	Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan;
18)	Pekeliling Kemajuan Pentadbiran Awam Bilangan 3 Tahun 2015 – Dasar Perkhidmatan Prasarana Kunci Awam Kerajaan [Government Public Key Infrastructure (GPKI)];
19)	Pekeliling Perbendaharaan Bil. 5 Tahun 2007 – Tatacara Pengurusan Aset Alih Kerajaan;
20)	Surat Pekeliling Am Bil. 2 Tahun 2000 - Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK);
21)	Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;
22)	Surat Pekeliling Am Bilangan 4 Tahun 2006 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

23)	Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009;
24)	Surat Pekeliling Perbendaharaan Bil.2 Tahun 1995 (Tambahan Pertama) - Tatacara Penyediaan, Penilaian dan Penerimaan Tender; (Dibatalkan oleh SPP 5/2007);
25)	Surat Pekeliling Perbendaharaan Bil. 3 Tahun 1995 - Peraturan Perolehan Perkhidmatan Perundingan;
26)	Surat Arahan Ketua Setiausaha Negara - Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) di Agensi-Agensi Kerajaan yang bertarikh 20 Oktober 2006;
27)	Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007;
28)	Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007;
29)	Surat Arahan Ketua Pengarah MAMPU – Pengaktifan Fail Log Server Bagi Tujuan Pengurusan Pengendalian Insiden Keselamatan ICT Di Agensi-Agensi Kerajaan yang bertarikh 23 Mac 2009;
30)	Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesenambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010;

	DASAR KESELAMATAN ICT PENTADBIRAN KERAJAAN NEGERI SEMBILAN	Versi
		3.0
		Tarikh
		12 Feb 2019

31)	Surat Arahan Ketua Pengarah Perkhidmatan Awam – Tindakan Ke Atas Penjawat Awam Yang Mendedahkan/Membocorkan Dokumen/Maklumat Terperingkat Kerajaan yang bertarikh 28 Januari 2015;
32)	Surat Arahan MAMPU.BDPICT(S) 700-6/1/3(21) bertarikh 19 November 2009 – Penggunaan Media Jaringan Sosial di Sektor Awam;
33)	Garis Panduan Keselamatan MAMPU 2004;
34)	Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS) 2002;
35)	Pekeliling Kemajuan Pentadbiran Awam Bilangan 2 Tahun 2015 – Pengurusan Laman Web Agensi Sektor Awam;
36)	Pelaksanaan Pelaksanaan Pensijilan MS ISO/IEC 27001:2007 Dalam Sektor Awam bertarikh 24 November 2010;
37)	Panduan Keperluan dan Persediaan Pelaksanaan Pensijilan MS ISO/IEC 27001:2007 Dalam Sektor Awam bertarikh 24 November 2010;
38)	Pekeliling Perkhidmatan Bilangan 5 Tahun 2007 – Panduan Pengurusan Pejabat bertarikh 30 April 2007; dan
39)	Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) Versi 1.0, April 2016